70-534 Azure Exam Labs

|  |  |
| --- | --- |
| C:\Users\DSTOLT~1.NOR\AppData\Local\Temp\SNAGHTML104f74f.PNG  Version: 1.0.1  PowerShell & Data Entry File: <http://aka.ms/azlab2script>  [www.MicrosoftVirtualAcademy.com](http://www.MicrosoftVirtualAcademy.com)  Support & Corrections:ITCamp@Microsoft.com | **Lab 1: Building Foundation**  **Lab 2: Building Workloads**  **Lab 3: Working with Identity**  **Lab 4: Build Application & SQL**  **Lab 5: Deploy Data Access App**  **Lab 6: Backup to Azure Recovery Vault**  **Lab 7: Create Linux VM**  **Lab 8 Backup an Azure VM**  **Lab 9: Copy Files with AZCopy**  **Lab 10: Backup Windows Client/Server**  **Lab 11 Creating/Managing WebApps**  **Lab 12 Web App & SQL (Preview Portal)**  **Labs 13 Many More Labs: Many more labs available in the book and at ITProGuru.com**  ***http://ITProGuru.com/HOL*** |

**Thanks to our sponsors…**

|  |  |
| --- | --- |
|  |  |
|  |  |

Contents

[Lab Requirements 4](#_Toc431807076)

[Lab 0: Login to Azure Portal 4](#_Toc431807077)

[Lab 1: Building the Foundation 5](#_Toc431807078)

[Login to the Azure Portal 5](#_Toc431807079)

[Create a new virtual network and subnets for objects 5](#_Toc431807080)

[Create a new storage account from the Azure management portal 6](#_Toc431807081)

[Create a new service from the Microsoft Azure management portal 7](#_Toc431807082)

[Connect your PowerShell to Azure 7](#_Toc431807083)

[Lab 2: Building Workloads 9](#_Toc431807084)

[Deploy a domain controller in Microsoft Azure 9](#_Toc431807085)

[Explore the virtual machines and connect via RDP 11](#_Toc431807086)

[Migrate DC01 to the designated static IP subnet 11](#_Toc431807087)

[DC01 designated static IP – Preview Portal 12](#_Toc431807088)

[Create a new database server VM from the Microsoft Azure management portal 14](#_Toc431807089)

[Assign a new DNS server and subnet for the virtual network 15](#_Toc431807090)

[Lab 3: Working with Identity 16](#_Toc431807091)

[Create a new Azure Active Directory environment 16](#_Toc431807092)

[Create an Azure Active Directory Administrator account 16](#_Toc431807093)

[Set a password for your admin account 17](#_Toc431807094)

[Configure and test the AADSync Service 18](#_Toc431807095)

[Implementing Multi-Factor Authentication 21](#_Toc431807096)

[Testing Multi-Factor Authentication 22](#_Toc431807097)

[Lab 4: Building Application & SQL Workloads 24](#_Toc431807098)

[Create a new web server virtual machine from the Microsoft Azure management portal 24](#_Toc431807099)

[Configure SQL Server System Defaults 25](#_Toc431807100)

[Import and configure the testing database on SQL01 26](#_Toc431807101)

[Configure firewall ports for SQL01 27](#_Toc431807102)

[Confirm Connectivity to SQL01 From WEBFE01 28](#_Toc431807103)

[Lab 5: Building Application Workloads – Deploy Data Access App 30](#_Toc431807104)

[Configure endpoints for WEBFE01 30](#_Toc431807105)

[Configure firewall ports for WEBFE01 30](#_Toc431807106)

[Remotely enable Internet Information Services on WEBFE01 using Windows PowerShell 31](#_Toc431807107)

[Deploy and test the Contoso Data Access sample site 32](#_Toc431807108)

[Lab 6 Create a new Ubuntu Linux VM using the gallery 34](#_Toc431807109)

[Connect to the new Linux VM using SSH and RDP 34](#_Toc431807110)

[Lab 7 - Backup an Azure VM 36](#_Toc431807111)

[Create a Backup Vault 36](#_Toc431807112)

[Restore a Virtual Machine 38](#_Toc431807113)

[Lab 8 – Using Azure Backup 39](#_Toc431807114)

[Lab 9 – Copy Files with AZCopy 42](#_Toc431807115)

[Install AZCopy on your Local Machine 42](#_Toc431807116)

[Locating storage access key; Preparing to copy files 42](#_Toc431807117)

[Upload files from the file system to Blob storage 43](#_Toc431807118)

[Lab 10 - Backing up a Windows Client to Microsoft Azure Recovery Services Backup Vault 45](#_Toc431807119)

[Create a Backup Vault 45](#_Toc431807120)

[Download the vault credential file 47](#_Toc431807121)

[Registering your Windows Client machine 48](#_Toc431807122)

[Backup and restore from a Windows server or Windows client machine 52](#_Toc431807123)

[Lab 11 Creating and Managing Website & Services 59](#_Toc431807124)

[Creating new elements and services 60](#_Toc431807125)

[Managing allocated resources 63](#_Toc431807126)

[Lab 12 Creating a Web Site + SQL (Preview Portal) 67](#_Toc431807127)

[13 Many More Labs 78](#_Toc431807128)

[Dan Stolts Blog http://ITProGuru.com/HOL 78](#_Toc431807129)

[Capturing Custom Images Page 31 78](#_Toc431807130)

[ADAL and Visual Studio Page 71 78](#_Toc431807131)

[Configure Azure AD Application Proxy Page 82 78](#_Toc431807132)

[External Authentication with ASP.net Page 92 78](#_Toc431807133)

[Consuming Mobile Services Page 143 78](#_Toc431807134)

[Custom Web API Page 159 78](#_Toc431807135)

[Create Websites using Visual Studio Page 254 78](#_Toc431807136)

[Create Packages to Publish Page 271 78](#_Toc431807137)

[Azure Backup (PowerShell Notes) Page 343 78](#_Toc431807138)

[Getting Started with PowerShell Page 354 78](#_Toc431807139)

[PowerShell Working with Storage Page 359 78](#_Toc431807140)

[PowerShell Working with Websites page 360 78](#_Toc431807141)

[Workflows page 361 78](#_Toc431807142)

[GitHub 78](#_Toc431807143)

[Azure Training 78](#_Toc431807144)

[PowerShell DSC 78](#_Toc431807145)

[Revision History 79](#_Toc431807146)

# Lab Requirements

The following components are required to successfully complete this Hands-on Lab:

* A Microsoft Azure Account and Credentials
* A modern web-browser with HTML5 and Javascript enabled
* Remote Desktop Client connection software
* Internet connectivity
* Identification for building access
* 10” or larger screen recommended

In addition, this hands-on lab guide assumes that lab participants are comfortable with performing the steps involved in implementing Windows Server 2012 and Active Directory in an on-premises datacenter environment.

NOTE: If you have questions along the way, please make sure you read the guide directions carefully and completely. If you still have questions, feel free to ask today’s presenter for assistance!

***Note:*** You WILL NOT have time to complete all labs today. Please finish at home or office.

# Lab 0: Login to Azure Portal

Lab 0 - Login to the Azure Portal

In this task you will login into the Azure Portal to ensure your subscription is ready to go.

 Perform the following tasks:

1) Open a browser, and then navigate to http://manage.windowsazure.com.

2) Click PORTAL located at the top of the Microsoft Azure site.

3) Log in using your Microsoft Azure credentials for your Microsoft Azure subscription.

4) If this is your first time logging into your Azure management portal, close the WINDOWS AZURE TOUR.

# Lab 1: Building the Foundation

In this first lab of building a core IaaS in Microsoft Azure, you will create the core building blocks for your Azure services:

* Virtual Network
* Storage
* Cloud Service

The services mentioned above are the core tenants that provide a foundation for your applications, virtual machines and hybrid connectivity in Azure. Having this well thought out, provides a great architecture for all of your cloud services.

## Login to the Azure Portal

Perform the following tasks:

1. Open a browser, and then navigate to [**http://Manage.WindowsAzure.com**](http://Manage.WindowsAzure.com).
2. Click **PORTAL** located at the top of the Microsoft Azure site.
3. Log in using your Microsoft Azure credentials for your Microsoft Azure subscription.
4. If this is your first time logging into your Azure management portal, close the WINDOWS AZURE TOUR.

## Create a new virtual network and subnets for objects

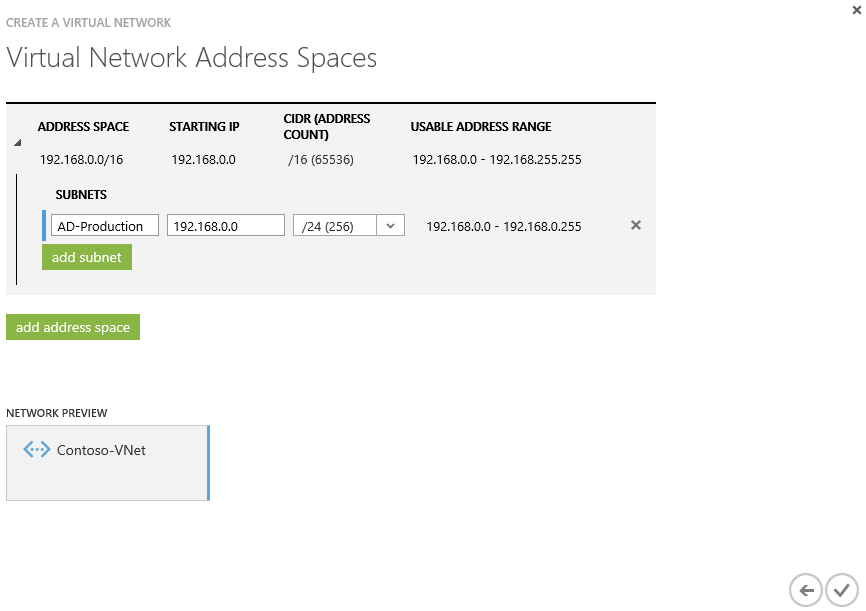
First, you will create a Microsoft Azure network object and corresponding subnet. Virtual Network lets you provision and manage virtual networks in Azure and, optionally, link them via secured VPN tunnels with your on-premises IT infrastructure to create hybrid and cross-premises solutions. With virtual networks, IT administrators can control network topology, including configuration of DNS and IP address ranges.   
You can use a virtual network to:

* Create a dedicated private cloud-only virtual network
* Securely extend your data center
* Enable hybrid cloud scenarios

With the virtual network you are creating will provide IP addresses assigned to objects and virtual machines you create in other labs that will be associated with this virtual network.  You will also leverage subnets to help organize your IP addresses as well.

Perform the following tasks in the **Azure management portal**.

1. In the Azure management portal (in the leftmost column), scroll to and click **NETWORKS**.
2. Click **NEW** (Plus “+” Sign) located at the bottom of the Azure management portal
3. Click **CUSTOM CREATE**.
4. In **NAME**, type **ITC-VNet** and then in **LOCATION**, select your closest location, and then click the **Next** arrow. ***(Important: Remember this choice. You will use the same Location for all options in all labs)***
5. Leave all **DNS** setting blank, and then click the **NEXT** arrow.
   * This network will initially use Azure DNS.
6. In **STARTING IP**, type **192.168.0.0**.
7. In **CIDR (ADDRESS COUNT)**, select **/16**.
8. Under **SUBNETS**, highlight **Subnet-1**, and then replace it with **AD-Production**.
9. Under **STARTING IP**, type **192.168.10.0**.
10. Under **CIDR (ADDRESS COUNT)** select **/24**.



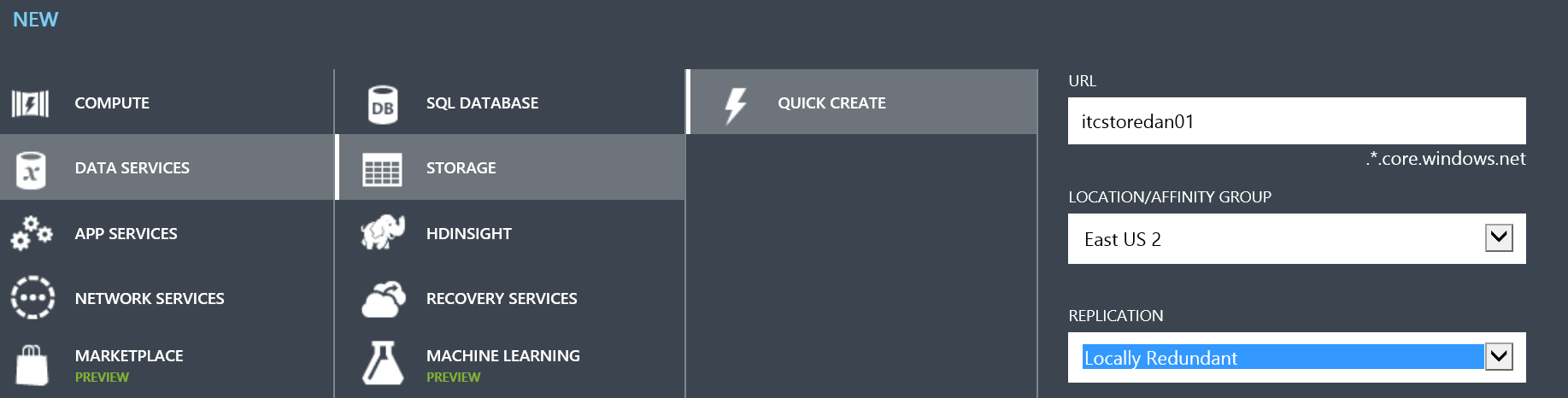
1. Under **SUBNETS**, click **add subnet**.
2. Replace **Subnet-1** with **AD-Production-Static**.
3. Set the **STARTING IP** to **192.168.11.0**.
4. Set the **CIDR (ADDRESS COUNT)** to **/24**.
5. Click the **Complete** icon (Check Mark).

## Create a new storage account from the Azure management portal

Microsoft Azure Storage is a massively scalable, highly available, and elastic cloud storage solution that empowers developers and IT professionals to build large-scale modern applications. Azure Storage is accessible from anywhere in the world, from any type of application, whether it’s running in the cloud, on the desktop, on an on-premises server, or on a mobile or tablet device. In this lab, you will create a storage account to contain all objects for your Azure services. Your VHDs, which you will create in lab 2 for your Azure virtual machines, will be stored in this storage account.

Perform the following tasks in the **Azure management portal**:

1. In the leftmost column, scroll to and click **STORAGE**.
2. Click **NEW (“+”)**, located at the bottom of the Azure management portal.
3. Make sure **STORAGE** is highlighted and click **QUICK CREATE**
4. In **URL**, type **itcstore<*Unique ID (can use your initials)>*** For example:   
   **itcstoredan01** ***(PLEASE NOTE: has to be all lowercase)***
5. In **LOCATION/AFFINITY GROUP**, select your closest datacenter region.



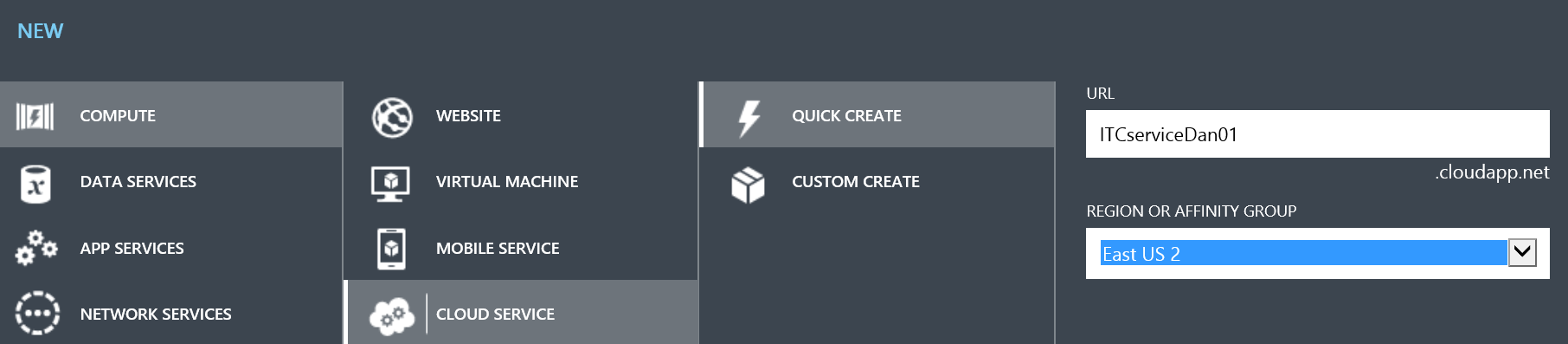
1. In **REPLICATION**, select **Locally Redundant**
2. Click **CREATE STORAGE ACCOUNT**.

## Create a new service from the Microsoft Azure management portal

By creating a cloud service, you can deploy a multi-tier application in Azure, defining multiple roles to distribute processing and allow flexible scaling of your application. A cloud service consists of one or more web roles and/or worker roles, each with its own application files and configuration. Azure Websites and Virtual Machines also enable web applications on Azure. The main advantage of cloud services is the ability to support more complex multi-tier architectures. In this section you will create a new service to contain your virtual machines. By assigning your new VMs to this service, they will be able to communicate internally.

Perform the following tasks in the **Azure management portal**.

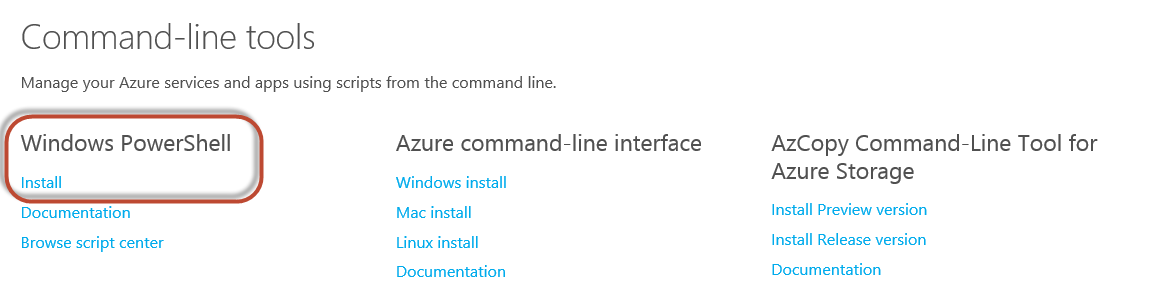
1. In the leftmost column, scroll to and click **CLOUD SERVICES**.
2. Click **NEW (“+”)** located at the bottom of the Azure management portal
3. Make sure **CLOUD SERVICE** is highlighted and click **QUICK CREATE**.
4. In **URL**, type **ITCservice<ID>**.  <*Unique ID (can use your initials)>* For example**:**  **ITCservicemh01   
   *NOTE: ID should be between 3-6 alpha-numeric. Must be unique in all of Azure (all customers/all accounts)***
5. In **REGION OR AFFINITY GROUP**, select your closest datacenter region



1. Click **CREATE CLOUD SERVICE**.

## Connect your PowerShell to Azure

Before you can manage virtual machines from PowerShell on your local administration station you need to download the tools. **Perform these actions from your local workstation/laptop.** If you cannot install on your laptop, you can come back and perform this lab from your DC and perform these steps on that VM.

1. In the Azure portal; click Azure the arrow next to Azure in the upper right corner of the portal then click downloads. You can also get to download directly by navigating to http://azure.microsoft.com/en-us/downloads/
2. Scroll down to Command-line tools section and under Windows PowerShell, click **Install** 
3. When prompted click **run** and follow the installation prompts
4. After installation is complete, In your Start Screen or Start Menu locate Microsoft Azure PowerShell and start it.
5. You will now need to connect Microsoft Azure PowerShell to your Azure subscription. In your PowerShell session type the following command:

**Add-AzureAccount**

Press <ENTER>

1. Enter your Azure Subscriber ID and Password.

NOTE: If you do not know your SubscriberID: Login to the Azure portal http://manage.windowsazure.com click on your **email address in the upper right corner**, Click **View My Bill.** This will list all subscriptions for the current logged in user. Click on the **subscription** you want to use, then scroll down so see your **Subscription ID** listed on the right.

1. You are now ready to use Azure Cmdlets with your subscription.

**IMPORTANT NOTE**: if this procedure does not work or you have any issues, you can try to use certificate authentication. Detailed step-by-step instructions can be found in the Appendix of this lab guide.

**End of Lab 1: Building the Foundation**

# Lab 2: Building Workloads

Azure virtual machines give you the flexibility of virtualization without spending the time and money to buy and maintain the hardware that hosts the virtual machine. However, you do need to maintain the virtual machine -- configuring, patching, and maintaining the operating system and any other software that runs on the virtual machine. In this lab you are going to deploy 2 virtual machines into Azure for the two workloads of identity and database. You will create these two virtual machines:

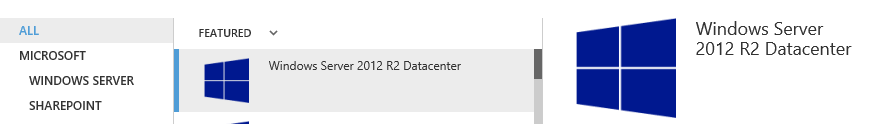
* A Domain Controller (DC01)
* A SQL Server (SQL01)

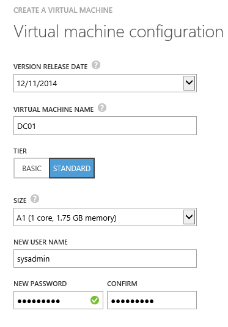
## Deploy a domain controller in Microsoft Azure

In this task, you will deploy a new virtual machine(VM) to function as a domain controller in your newly created virtual network created in Lab01. As you provision the VM you will leverage a custom script extension to install Active Directory as a part of the provisioning process. Custom Script Extensions can automatically download scripts and files from Azure Storage and launch a PowerShell script on the VM. These scripts can be used to install additional software components, and in this lab you will use it to install Active Directory. Like the any other VM extensions, Custom Script Extensions can be added during VM creation or after the VM has been running. During the last portion of the lab you will also configure the AD service as the DNS server for the virtual network you created in Lab 1, and you’ll assign it a static IP Address(technically speaking this is a DHCP reservation in the subnet but it will be referred to as a static IP pretty much everywhere in Azure documentation.)

Perform the following tasks in the **Azure management portal**.

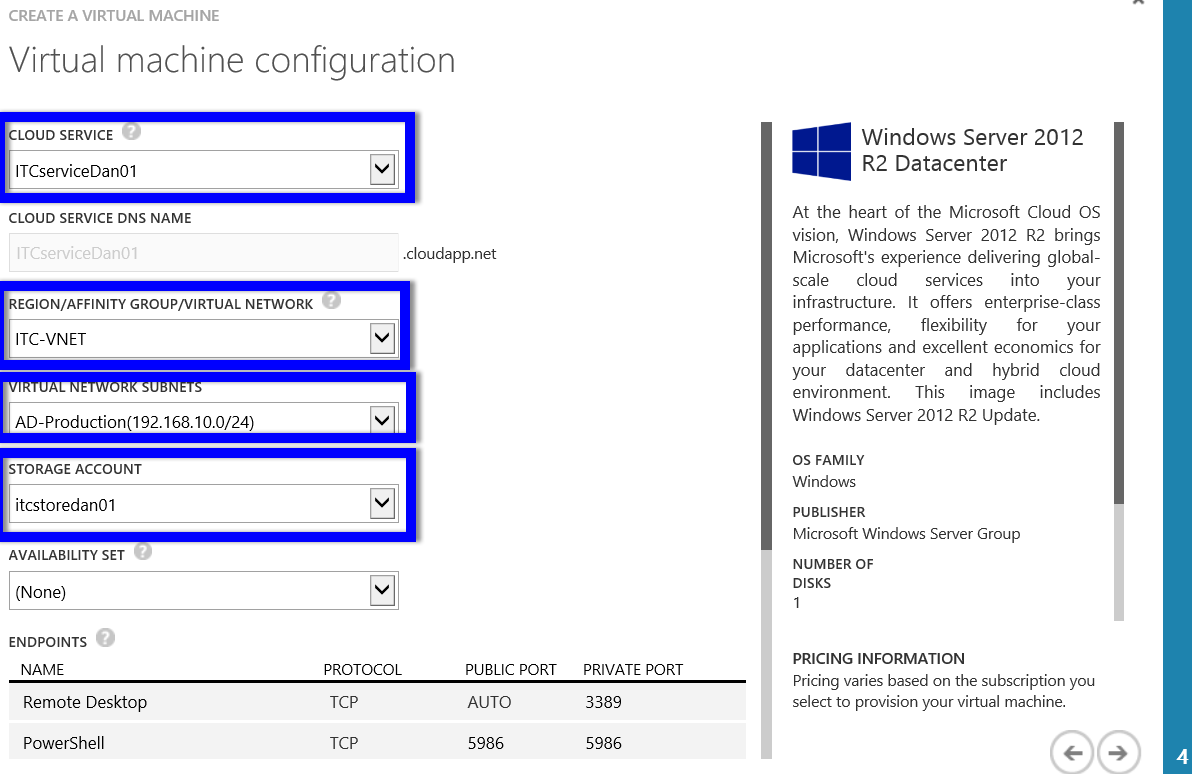
1. In the Azure management portal, click **VIRTUAL MACHINES**.
2. Click **NEW** (Plus “+” Sign) located at the bottom of the Azure management portal
3. Click **COMPUTE**, click **VIRTUAL MACHINE**, and then click **FROM GALLERY**.
4. In **Choose an Image**, click **Windows Server 2012 R2 Datacenter**, and then click the **Next** arrow.



1. Create a new virtual machine using the values in the following table.  Please note: You can user your own username and password, just make sure to remember it!

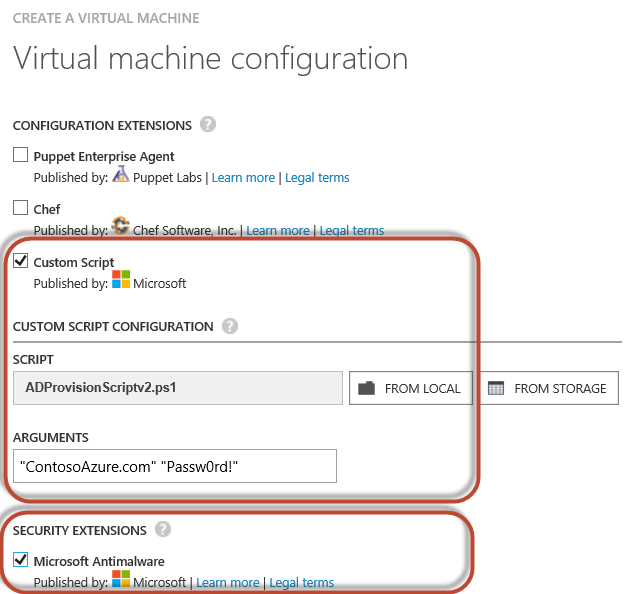
|  |  |
| --- | --- |
| Property | Value |
| VIRTUAL MACHINE NAME | DC01 |
| TIER | Standard |
| SIZE | A1 |
| USER NAME | SysAdmin |
| NEW PASSWORD and CONFIRM | Passw0rd! |

1. then click the **Next** arrow
2. On the Virtual machine configuration page 3, in **CLOUD SERVICE**, select **itcservice<ID>.** (From Lab 1)
   * ITC-VNet will be automatically selected. If you do not have ITC-VNet available, you likely have the ITC-VNet in a different Location. Go back and fix location to make sure it’s the same.
3. In **STORAGE ACCOUNT**, select **itcstore<ID>**  (From Lab 1)
   * If your storage account is not in the list, you may have to cancel out of this wizard, wait a few minutes for it to finish building, and try again.
4. In **REGION/AFFINITY GROUP/VIRTUAL NETWORK**, verify that **ITC-VNet** is selected.
5. In **VIRTUAL NETWORK SUBNETS** , verify that **AD-Production (192.168.10.0)/24** is selected, and then click the **Next** arrow.



1. In a separate tab or window: Download **http://ITProGuru.com/downloads/ADProvisionScriptv2.txt** to your local machine. ***Make sure you*** *Click on File>Save As.. and* ***save it as*** **ADProvisionScriptv2.ps1**. Make a note of where you put it. It will be needed for the next step.
2. On the Virtual machine configuration page, under **Configuration Extensions**, check **Custom Script.**
3. Click **FROM LOCAL,** Navigate to the **ADProvisionScriptv2.ps1** file you download above click **Open**
4. In the **Arguments** field type the following (including quotation marks, the password can change to match the one you gave in step 5 if you did not use the lab’s recommended password):

**"ContosoAzure.com" "Passw0rd!"**

**This password sets the –SafeModeAdministratorPassword for Active Directory by the way.**

1. On the Virtual machine configuration page, under Security Extensions, check **Microsoft Antimalware**.
2. Click the **Complete** icon.
   * The virtual machine will take a few minutes to create. Depending on the load this may take between 5 and 25 minutes.
   * You will return to complete the rest of the DC networking configuration at the end of the lab
3. **NOTE:** After the domain is created; you will have to login with a domain user **ConstosoAzure\sysadmin** instead of DC01\sysadmin
4. **NOTE:** if you already started the install and missed the Execute Script part, see the appendix for PowerShell instructions for adding AD to the DC

## Explore the virtual machines and connect via RDP

Now that the virtual machine is created, you want to log on and verify that it looks, feels, and behaves just like any server on your network.

Perform the following tasks in the **Azure management portal**.

1. On the left menu of the Azure management portal, scroll to and click **VIRTUAL MACHINES**.
2. Next to **DC01**, click the **DNS Name** to open the **Service dashboard**.
3. Click **DASHBOARD**.
   * You can review information about the running virtual machines, as well as view the current health.
4. Click **MONITOR**.
   * You can view performance and data statistics.
5. Click **INSTANCES**.
6. Click **DC01** to open the VM dashboard.
7. Click **DASHBOARD**.
   * You can review information about the running virtual machines, as well as view the current health.
8. Click **MONITOR**.
   * You can view performance and data statistics.
9. Click **ENDPOINTS**.
   * You can configure published endpoints, which are similar to firewall rules, to allow applications to access services running on the VM.
10. Click **CONFIGURE**.
    * You can modify the properties of the virtual machine. You can also configure monitoring from multiple locations to ensure your endpoint is operational.
11. Click **DASHBOARD**.
12. On the bottom bar, click **CONNECT**, and then click **Open**.
13. Click **Connect**.
14. When prompted, log on as **ContosoAzure\sysadmin** using **Passw0rd!** as the password. (Substitute the username and password you used during VM Creation if different than the lab recommendations.)
15. Click **Yes**.
    * You are now logged on to your newly created virtual machine.
16. Click **No** when prompted to enable discovery of devices.

## Migrate DC01 to the designated static IP subnet

In this task, you will move DC01 to the designated static IP subnet. You will then configure a static IP address. When you assign static IP addresses it is highly recommended you also provision a dedicated subnet for the static machines, which is why we already handled this in Lab01

You can accomplish what we’re about to do in two separate ways – PowerShell, or the new Azure Preview Portal. For our Lab, we’re going to use PowerShell, and then show you where it can be found and configured in the new portal.

Perform the following tasks on your workstation using PowerShell

NOTE: You will need to make sure you have installed the Microsoft Azure PowerShell cmdlets and connect it (or authenticate) to your subscription. You can read the **Install PowerShell Tools** section for more information.

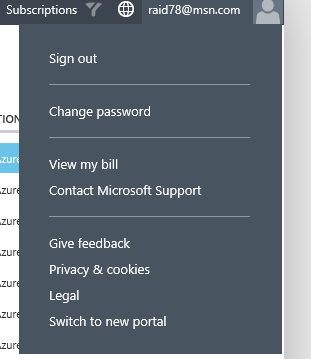
1. Open **Azure PowerShell**.
2. To test the pending static IP for availability, type the following command (on one line), and then press **ENTER**.
   * **Test-AzureStaticVNetIP –VnetName ITC-VNet –IPAddress 192.168.11.100**
   * The output of True indicates this address is available. An output of false indicates the address is assigned, and will also provide a list of available IP addresses.
3. To migrate the VM, type the following command (all on one line) and then press **ENTER**. Replace **<ID>** with your unique ID.
   * **Get-AzureVM -Name DC01 -ServiceName itcservice<ID> | Set-AzureSubnet -SubnetNames AD-Production-Static | Update-AzureVM**
4. To verify the VM has been migrated, type the following command, and then press **ENTER**. Replace **<ID>** with your unique ID.
   * **Get-AzureVM -Name DC01 –ServiceName itcservice<ID>**
   * Note the value of IPAddress and PowerState. The VM should have a new IP address on your new subnet, and be starting.
5. To assign the desired static IP, type the following command (on one line), and then press **ENTER**. Replace **<ID>** with your unique ID.
   * **Get-AzureVM -Name DC01 –ServiceName itcservice<ID> | Set-AzureStaticVNetIP –IPAddress 192.168.11.100 | Update-AzureVM**
6. To verify the VM has been configured, type the following command, and then press **ENTER**. Replace **<ID>** with your unique ID.
   * **Get-AzureVM -Name DC01 –ServiceName itcservice<ID>**
   * Note the value of **IPAddress** and **PowerState**. The VM should have the assigned static IP on your new subnet, and be starting.

Before proceeding to the next step you may need to wait for the last operation to complete. ***Assigning a new IP address forces the VM to restart.*** Now let’s take a look at where we can configure IP addressing using the New Preview Portal.

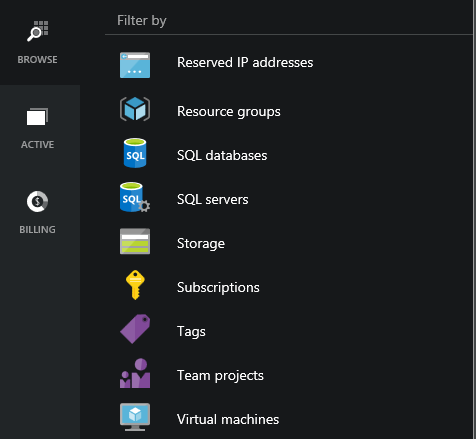
## DC01 designated static IP – Preview Portal

While the new portal offers some great enhancements to managing Azure. It is still in preview, while this task will give you a glimpse into the new portal, there is one thing you cannot currently do when setting a static IP address: Setting a separate subnet. You can still do it, but you have to leverage PowerShell.

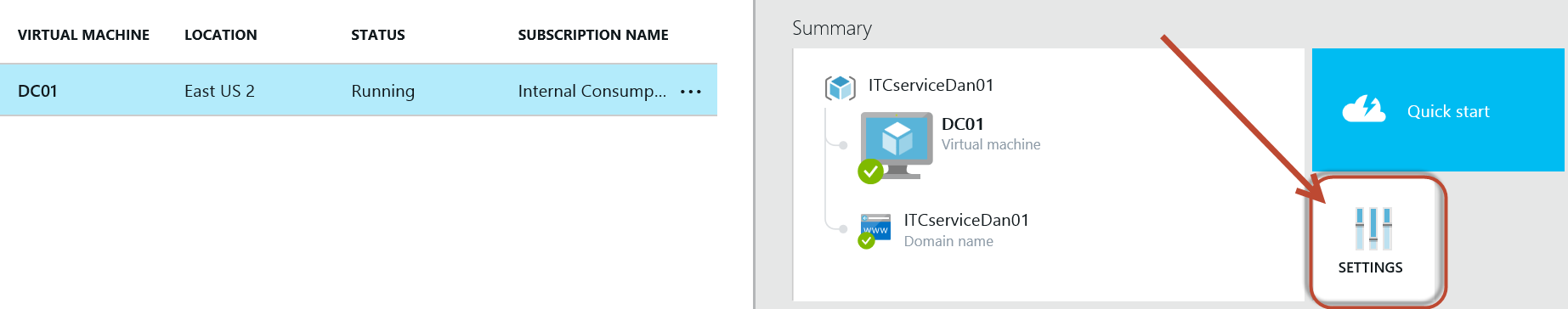
1. In the Azure management portal, click on your **Account ID** **e-mail** **address** in the upper right hand corner and click on **Switch to new portal.** Notice a new tab automatically opens



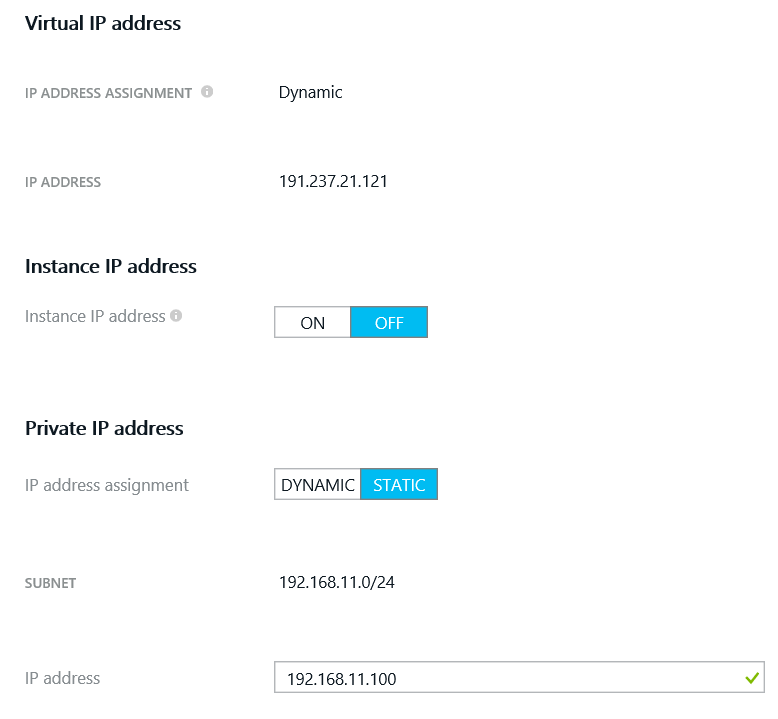
1. If prompted for your credentials, enter your ID and password to enter the new portal
2. On the left hand toolbar in the portal click **Browse** and scroll to and select **Virtual machines**



1. In the Virtual machine list select **DC01**
2. In the **DC01** journey pane select **SETTINGS**



1. In the **SETTINGS** options select **IP addresses**
2. In the **IP addresses** journey, NOTE that the Private IP address is set to Static. If it hadn’t already been set that way, we could have changed it here.
3. NOTE that the **IP address** is **192.168.11.100**,just as we had set using PowerShell. If we wanted to, we could change it here and click **Save** up above.



You may now close the new preview portal tab.

## Create a new database server VM from the Microsoft Azure management portal

In this task, you will create a database server to run the database portion of the application. This will be a SQL Server Enterprise 2014 VM.  You will leverage one of the many virtual machine images that are located in the virtual machine gallery. Images are used in Azure to provide a new virtual machine with an operating system. An image might also have one or more data disks. Images are available from several sources:

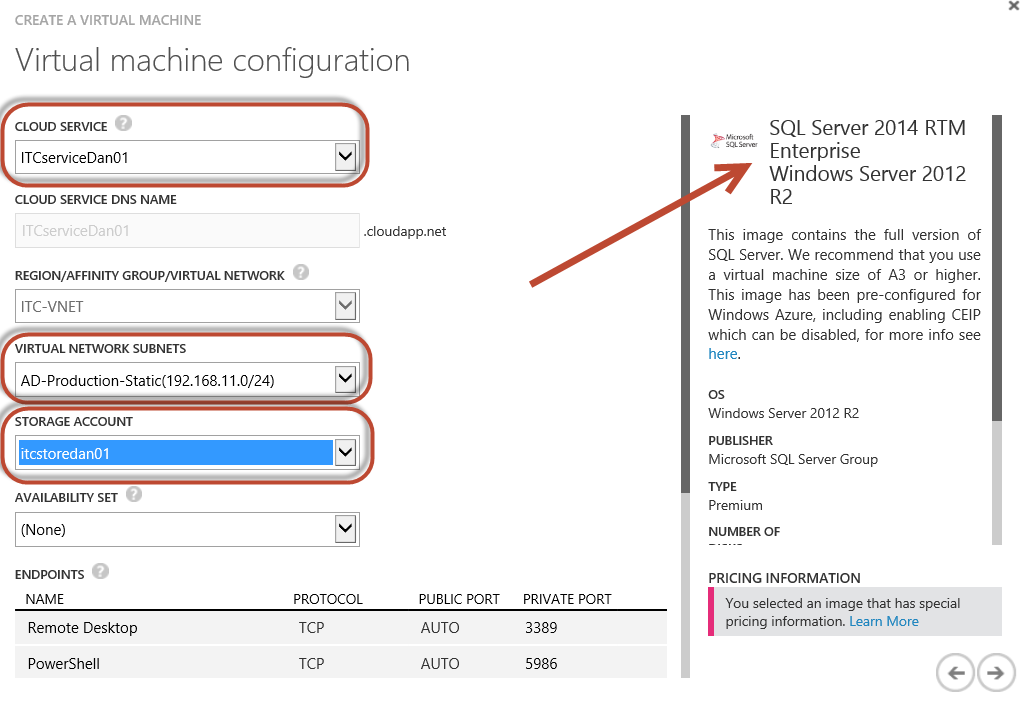
* Azure offers a gallery of images -- recent versions of Windows Server and several distributions of the Linux operating system. Some images also contain applications, such as SQL Server. MSDN Benefit and MSDN Pay-as-You-Go subscribers have access to additional images.
* The open source community offers images through VM Depot.
* You can store your own images in Azure, by either capturing an existing Azure virtual machine for use as an image or uploading an image.

Perform the following tasks in the non-preview **Azure management portal**.

1. Click **NEW (“+”)**, located at the bottom of the Azure management portal.
2. Click **COMPUTE**, click **VIRTUAL MACHINE**, and then click **FROM GALLERY**.
3. In **Choose an Image**, click **SQL Server**, and   
   find and select **SQL Server 2014 RTM Enterprise**. Click the **Next** arrow.
4. Create a new virtual machine using the values in the following table, and then click the **Next** arrow.

|  |  |
| --- | --- |
| Property | Value |
| VIRTUAL MACHINE NAME | SQL01 |
| TIER | Standard |
| SIZE | A3 |
| NEW USER NAME | SysAdmin |
| NEW PASSWORD and CONFIRM | Passw0rd! |

1. On the Virtual machine configuration page, in **CLOUD SERVICE DNS NAME**, select **itcservice<ID>** (where <ID> is your unique ID).
2. In **STORAGE ACCOUNT**, select **itcstore<ID>**
3. In **REGION/AFFINITY GROUP/VIRTUAL NETWORK**, select **ITC-VNet**.
4. In **VIRTUAL NETWORK SUBNETS** select **AD-Production-Static (192.168.11.0)/24**,
5. In **STORAGE ACCOUNT** Select **itcstore<ID>**



1. Then click the **Next** arrow.
2. On the Virtual machine configuration page, under **Security Extensions**, check **Microsoft Antimalware**.
3. Click the **Complete** icon.
   * The virtual machine will take a several minutes to create. Depending on the load this may take between 15 and 35 minutes.
   * You will return to complete the rest of the SQL configuration in an up-coming lab.

## Assign a new DNS server and subnet for the virtual network

In this task you will create a new DNS server entry. This entry will be assigned to all computers using DHCP on their next restart, since all VMs use DHCP in Azure, even the ones with “static IPs” as these are technically just DHCP reservations on the VNet. Azure provides automatic routing between subnets on the same virtual network, but automatic name resolution only when machines are in the same Cloud Service.  *Though we won’t be doing so in these labs, if we were to add new VMs to the domain, they would have entries in DNS, so that it wouldn’t matter what cloud service they were in. They’d have name resolution through DNS on the Domain Controller.*

*URGENT NOTE: Please confirm that the creation of the domain is complete on DC01 BEFORE changing DNS. You can do this by looking in Server Manger on DC01, AD DS and DNS should both be listed in the left NAV. If you do not, name resolution will fail*

Perform the following tasks in the non-preview **Azure management portal**.

1. In the Azure management portal, click **NETWORKS**.
2. Click **ITC-VNet**
3. Click **CONFIGURE**.
4. In **dns servers**, type **DC01**, and then in IP ADDRESS, type **192.168.11.100**.
5. Click **Save**.

# Lab 3: Working with Identity

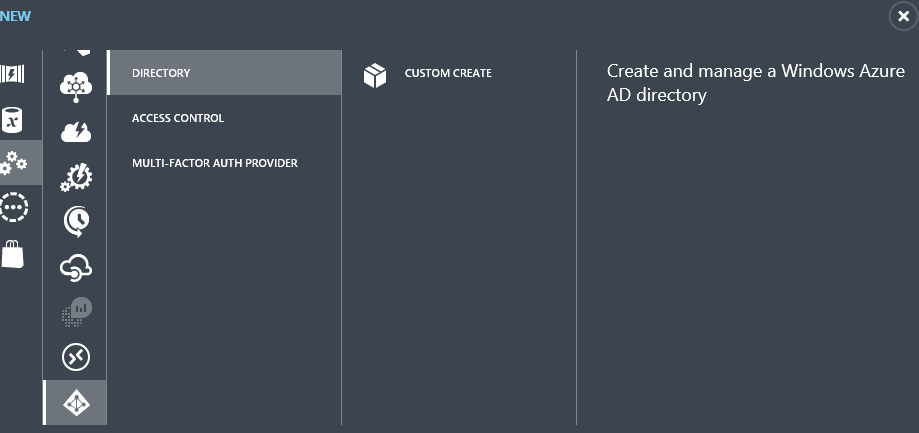
Azure Active Directory is a service that provides identity and access management capabilities in the cloud. In much the same way that Active Directory is a service made available to customers through the Windows Server operating system for on-premises identity management, Azure Active Directory (Azure AD) is a service that is made available through Azure for cloud-based identity management. Azure AD can be used as a standalone cloud directory for your organization, but you can also integrate existing on-premises Active Directory with Azure AD. Some of the features of integration include directory sync, password sync and single sign-on, which further extend the reach of your existing on-premises identities into the cloud for an improved admin and end user experience.

## Create a new Azure Active Directory environment

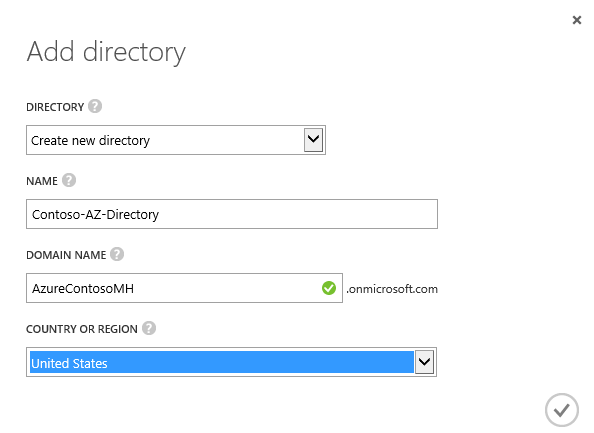
In this task, you will create a new Azure Active Directory tenant.

Perform the following tasks in the **Azure management portal**.

1. In the Azure management portal, click **ACTIVE DIRECTORY**.
2. Click **NEW**, click **APP SERVICES**, click **ACTIVE DIRECTORY**, click **DIRECTORY**, and then click **CUSTOM CREATE**.



1. In **NAME**, type **Contoso-AZ-Directory**.
2. In **DOMAIN NAME**, type **AzureCONTOSO<ID>** (where <ID> is your unique ID).
3. In **COUNTRY OR REGION**, select **UNITED STATES**, and then click the **Complete** icon.
   * If you are not in the United States, select it anyway to ensure the consistency of the lab steps.

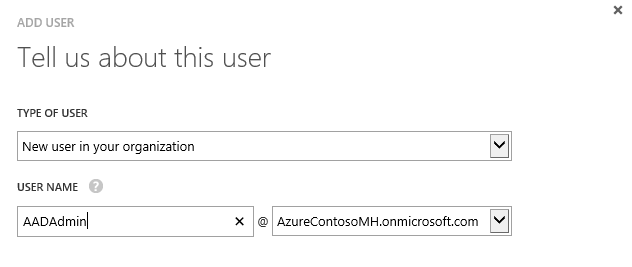


## Create an Azure Active Directory Administrator account

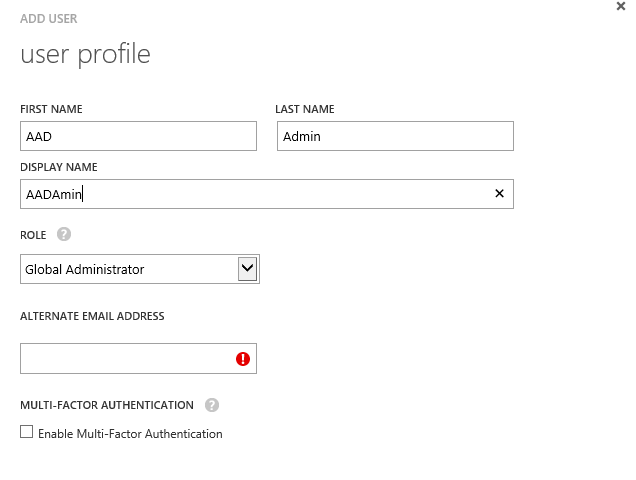
In this task, you will create a user account to serve as the administrator of your Azure Active Directory service.

Perform the following tasks in the **Azure management portal**.

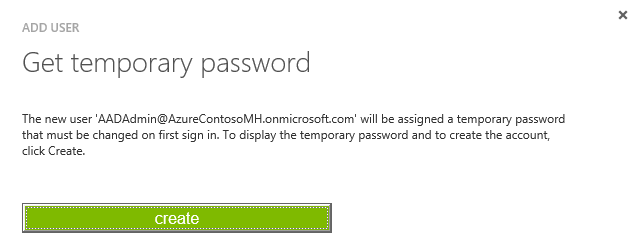
1. In the Azure management portal, click **ACTIVE DIRECTORY**, and then click **Contoso-AZ-Directory**.
2. Under **Contoso-AZ-Directory**, click **USERS**, located on the top menu.
3. In the bottom bar, click **ADD USER**.
4. In **USER NAME**, type **AADAdmin**, and then click the **Next** arrow.



1. In **FIRST NAME**, type **AAD**, and then in Last Name, type **Admin**.
2. In **DISPLAY NAME**, type **AADAdmin**.
3. In **ROLE**, select **Global Administrator**.
4. In **ALTERNATE EMAIL ADDRESS**, type any valid e-mail address you have access to, and then click the **Next** arrow.



1. Under **Get temporary password**, click **create**.



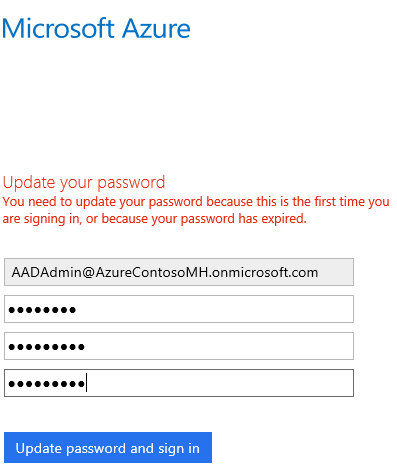
1. **MAKE NOTE** **of this password** as you will need it later.
2. Click the **Complete** icon.
3. Note the **USER NAME** value of the user; you will need this later.
   * The USERNAME value will be based on the account you used to manage Microsoft Azure.

## Set a password for your admin account

In this task, you will perform an initial logon to set the password for the admin account.

Perform the following tasks on your **local** workstation.

1. Close out of all web browser sessions. Using **Internet Explorer**, navigate to **manage.windowsazure.com**.
2. Log in as **AADAdmin** using the Unique <ID> and password you noted previously. i.e. [AADAdmin@AzureContoso<ID>.onmicrosoft.com](mailto:AADAdmin@AzureContoso%3cID%3e.onmicrosoft.com)
   * You will need to use the username value you noted earlier.
   * You may need to sign out first.
3. When prompted, change the password to **Passw0rd!** and then click **Update password and sign in**.
   * You will see a message “No subscriptions found.” This is expected. The user is not permitted to manage subscription level details.



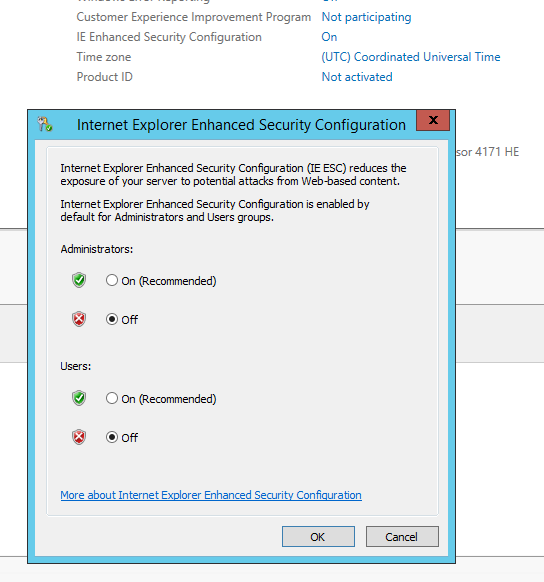
1. Close **Internet Explorer**.

## Configure and test the AADSync Service

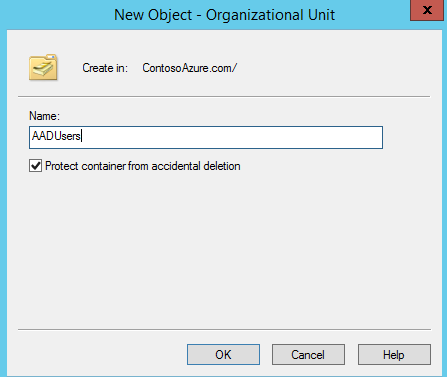
In this task, you will configure Windows Server 2012 R2 and create a new user to test your synchronization when you enable DirSync, and then perform an initial sync to populate your Azure Active Directory service with copies of your local user accounts.

Connect using RDP to **DC01**:

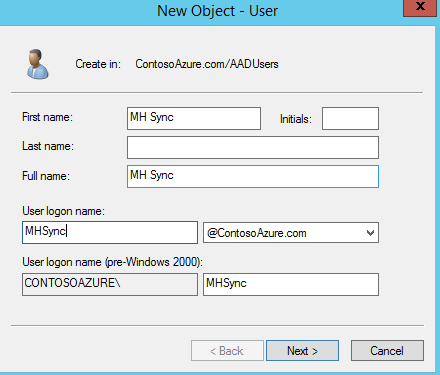
1. Close all web browsing sessions then reopen Internet Explorer and navigate to [**http://Manage.WindowsAzure.com**](http://Manage.WindowsAzure.com).
2. Log in with your Microsoft account used in the previous labs, **not** the AD administrator account from the previous section.
3. On the left menu of the Azure management portal, click **VIRTUAL MACHINES**.
4. Next to **DC01**, click the **DC01** computer name to open the Virtual Machine Quick Start or Dashboard.
5. Click **DASHBOARD**.
6. On the bottom bar, click **CONNECT**, and then click **Open**.
7. Click **Connect**.
8. When prompted, log on as **sysadmin** using **Passw0rd!** as the password.
9. Click **yes**.
   * You are now logged on to your virtual machine.
10. Open **Server Manager** and click **Local Server** on the left hand navigation pain.
11. Click on **IE Enhanced Security Configuration** and click **on**.
12. In the **Security Configuration** screen click **off** for both **administrators** and **users**. This is just for testing in this lab.
13. Click **OK**.



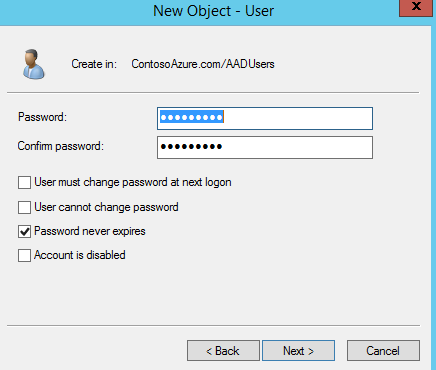
1. In **Server Manager** click **tools** and select **Active Directory Users and Computers**
2. Right click on **ContosAzure.com** and select **New -> Organizational Unit**
3. In the name type **AADUsers** and click **OK**



1. Right click on **AADUsers** and select **New User**
2. In **name** user your unique <ID> from earlier followed by sync for the logon name for example MHSync. Click **Next**



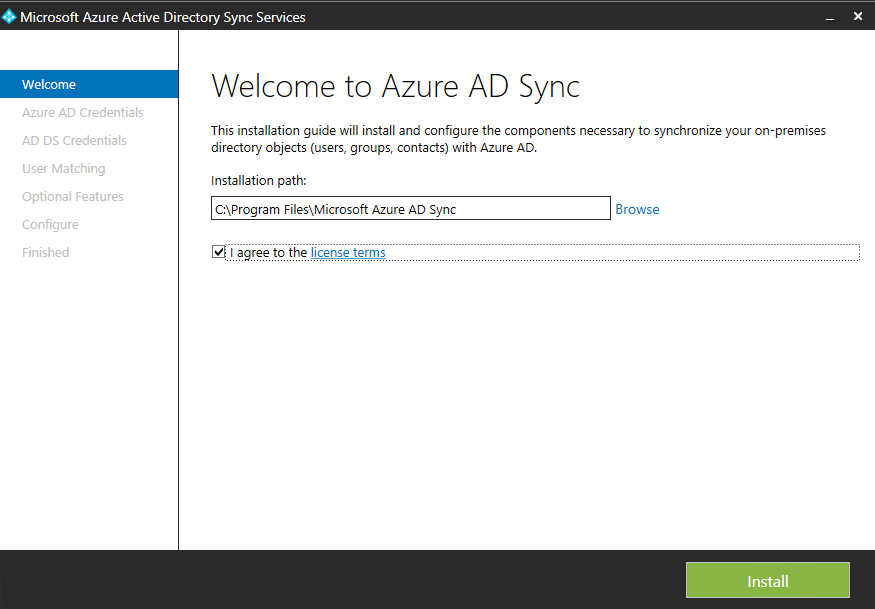
1. On the **password** screen enter a password, **Passw0rd!** and check the box **Password never expires**. Click **Next**.



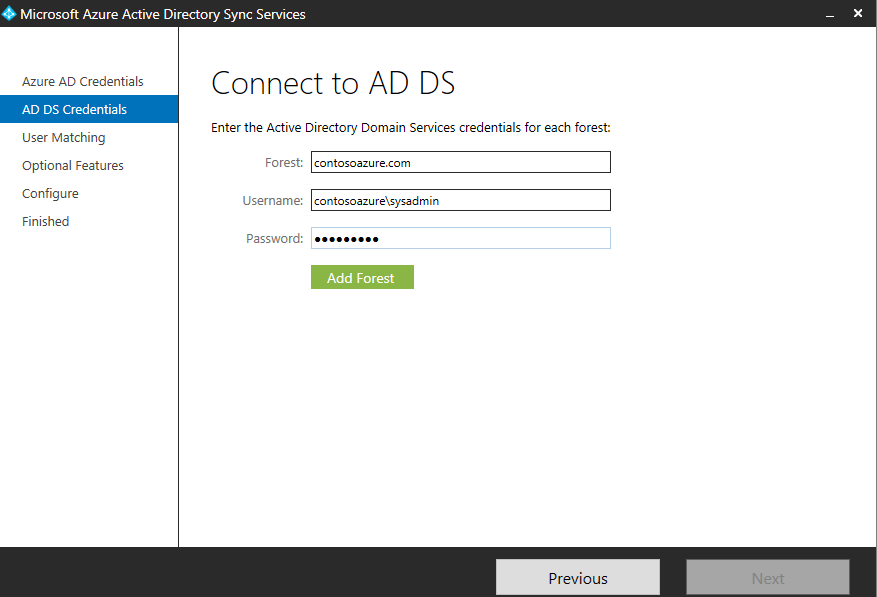
1. Review the new user and click **Finish**.
2. Still on **DC01**: Using **Internet Explorer**, navigate to [**http://**Azure.Microsoft.com](http://manage.windowsazure.com)
3. Log in as your subscription user, not the user you just created
4. In the Azure management portal, scroll to and click on **ACTIVE DIRECTORY**.
5. Click **Contoso-AZ-Directory**, and then click **Directory Integration**.
6. Next to **DIRECTORY SYNC**, click **Activated**.
7. Click **Save**, and then click **Yes**
   * Wait for the job to complete before proceeding.



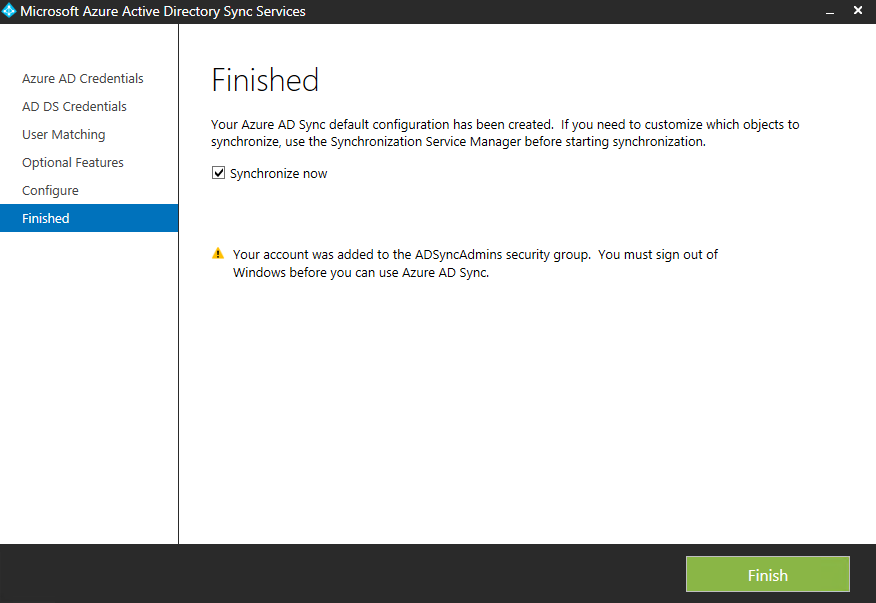
1. Using **Server Manager** – Add Feature .Net Framework 3.5 and 4.5  
   **NOTE:** .Net Framework may take about 5 minutes or longer to install.
2. Open **Internet Explorer** and go to [**http://aka.ms/azureadsync**](http://aka.ms/azureadsync) to download the **Microsoft Azure Active Directory Sync Services**
3. Click **download**
4. Save the tool to your **desktop**.
5. On the desktop, right click on the **MicrosoftAzureADConnectionTool** and select **Run As Administrator**. This will install and configure the tool.
6. Check the **I agree to the terms** and click **Install**

  
 **NOTE:** dirSync may take about 10 minutes or longer to install.

1. In **User name**, type [**AADAdmin@AzureContoso<ID>.onmicrosoft.com**](mailto:AADAdmin@AzureContoso%3cID%3e.onmicrosoft.com), replacing **<ID>** with the unique ID for your domain name.
2. In **Password**, type **Passw0rd!** and then click **Next**.
3. In the **Forest** type in **ContosoAzure.com**
4. In **User name**, type **contosoazure\sysadmin**.
5. In **Password**, type **Passw0rd!** and then click **Add Forest**
6. Click **Next**.



1. On **User Matching**, leave the defaults and click **Next**
2. On **optional features** select **Password synchronization** and click **Next**
3. On the **Configure** screen review the options and click **Configure**..
4. When configuration has completed review the screen, verify **Synchronize now** is selected and then click **Finish**.



1. Switch to your Azure management portal, and then click **ACTIVE DIRECTORY**.
2. Click the **Domain that synchronized**, and then click **Users and look for the user you created earlier**
   * You should eventually see the user you created in AD on DC01 now having been synchronized to your Azure Active Directory.

## Implementing Multi-Factor Authentication

Multi-factor or two-factor authentication is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It works by requiring any two or more of the following verification methods:

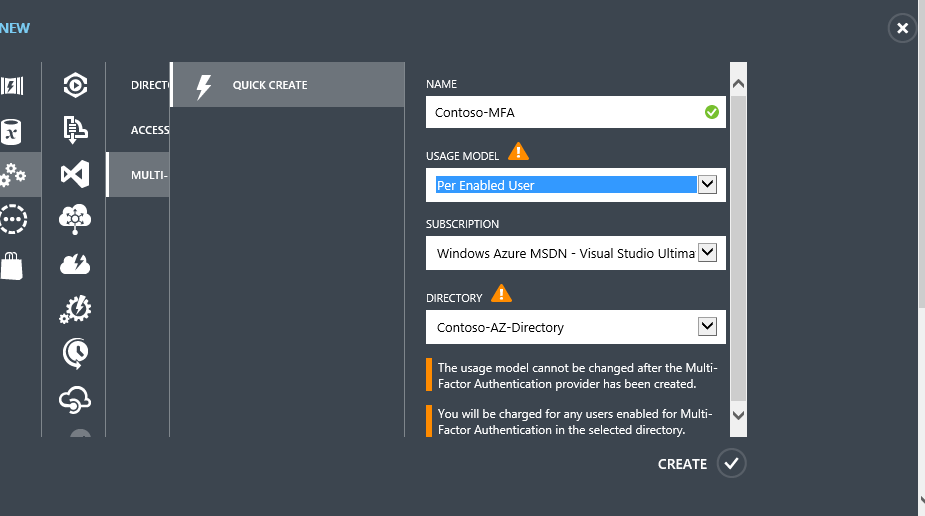
* Something you know (typically a password)
* Something you have (a trusted device that is not easily duplicated, like a phone)
* Something you are (biometrics)

The security of multi-factor authentication lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Conversely, if the user happens to lose the device, the finder of that device won't be able to use it unless he or she also knows the user's password. Azure Multi-Factor Authentication is the multi-factor authentication service that requires users to also verify sign-ins using a mobile app, phone call or text message. It is available to use with Azure Active Directory, to secure on-premise resources with the Azure Multi-Factor Authentication Server, and with custom applications and directories using the SDK.

In this task, you will configure Multi-Factor Authentication (MFA) with Microsoft Azure. To complete this module fully, you need to have a phone which can send and receive text messages or calls. You will configure this lab to use your phone as a second authentication factor this is done via replying to a system-generated text or voice message.

We will start by enabling the MFA service

1. Using Internet Explorer, navigate to **manage.windowsazure.com**.
2. Log on using your tenant account.
3. In Microsoft Azure, click **ACTIVE DIRECTORY**.
4. Click **MULTI-FACTOR AUTH PROVIDERS**, and then click **CREATE A NEW MULTI-FACTOR AUTHENTICATION PROVIDER**.
5. In NAME, type **Contoso-MFA**, ensure the correct subscription is selected (If you have multiple subscriptions tied to your live ID).
6. For directory select Contoso-AZ-Directory and then click **CREATE**.



## Testing Multi-Factor Authentication

In this task, you will test multi-factor authentication. Ensure you have the phone readily available as you will have a limited time to receive and reply to the text message generated by Microsoft Azure.

Perform this task on your **local machine**.

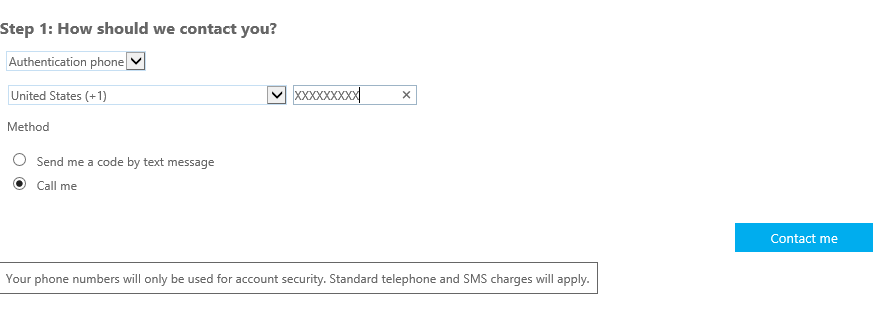
1. In the Microsoft Azure active directory portal click **directory** and click **Contoso-AZ-Directory**.
2. On the top bar click **Configure**
3. Under the **multi-factor authentication** section click **Manage Service Settings**



1. If prompted enter your tenant credentials
2. In **multi-factor authentication** click **users** on the top navigation bar.
3. Select the User you created earlier and click **Enable** under quick steps



1. On the information screen, review the message and click **enable multi-factor auth**.
2. Click **Close**
3. Open a new tab in **Internet Explorer** and navigate to <http://aka.ms/MFASetup> ***Note: If you are signed in, sign out to continue***
4. On the **Sign in** screen type in the username and password you created earlier and click sign in.
5. Since this is the first time the user has logged in you will need to configure MFA, click **Set it up now**
6. Fill in your contact information (phone number of your mobile phone), select the **Call me** radio button, and click **Contact me**



1. Answer your phone when it rings, and listen to the instructions. Press **#** to finish the authentication process. On the Additional security verification click **Done**.
2. Your sign-in process will continue and ***you will be called again***. Answer your call and type **#** to finish the logon process.

# Lab 4: Building Application & SQL Workloads

## Create a new web server virtual machine from the Microsoft Azure management portal

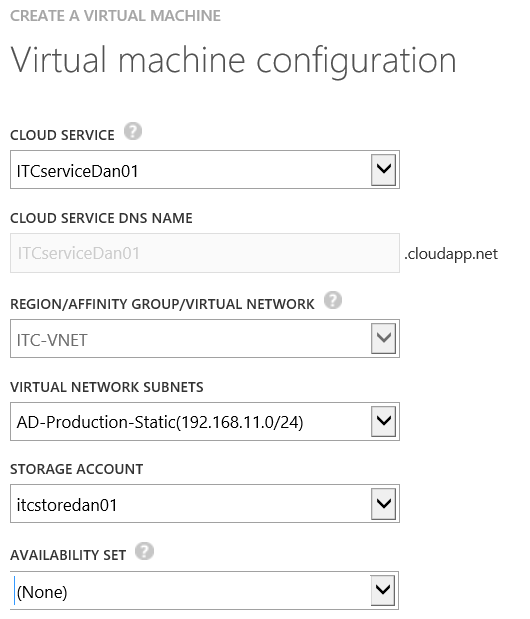
You will create a new virtual machine to run the web application. You can create this VM using quick create; however, that will not enable you to specify the service or storage, and will create separate storage and services for this VM. You will use the gallery option to ensure you can specify the storage and services for the VM.

Perform the following tasks in the **Azure management portal**:

1. Click **VIRTUAL MACHINES** located on the left menu of the Azure management portal.
2. Click **+New** to **CREATE A VIRTUAL MACHINE**.
3. Click **COMPUTE**, click **VIRTUAL MACHINE**, and then click **FROM GALLERY**.
4. In **Choose an Image**, click **Windows Server 2012 R2 Datacenter**, and then click the **Next** arrow.
5. Create a new virtual machine using the values in the following table, and then click the **Next** arrow.

|  |  |
| --- | --- |
| **Property** | **Value** |
| VIRTUAL MACHINE NAME | WEBFE01 |
| TIER | Standard |
| SIZE | A2 |
| NEW USER NAME | SysAdmin |
| NEW PASSWORD and CONFIRM | Passw0rd! |

1. On the Virtual machine configuration page, in **CLOUD SERVICE**, select **itcservice<ID>**.
2. In **STORAGE ACCOUNT**, select **itcstore<ID>.**
3. In **REGION/AFFINITY GROUP/VIRTUAL NETWORK**, verifity **ITC-VNet** is selected
4. In **VIRTUAL NETWORK SUBNETS** select **AD-Production-Static (192.168.11.0)/24**,

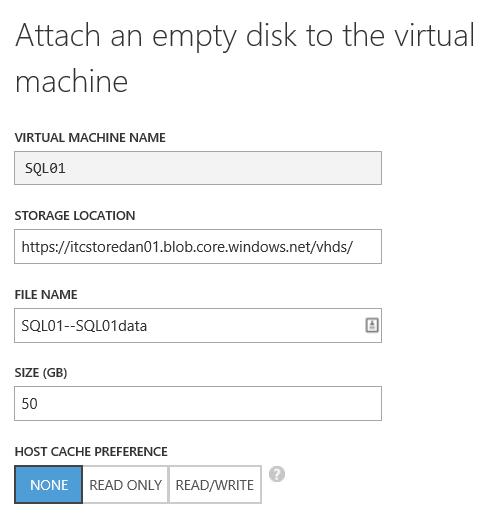


1. Click the **Next** arrow.
2. On the Virtual machine configuration page, under **Security Extensions**, check **Microsoft Antimalware**.
3. Click the **Complete** icon.
   * The virtual machine will take a few minutes to create. Depending on the load this may take between 5 and 25 minutes.
   * Wait for the new virtual machine to finish before proceeding.

## Configure SQL Server System Defaults

While the web server is being created, let’s go setup some defaults for SQL Server. You would never store SQL Data on a boot drive so the first thing we will do is add an additional drive that will be used for the SQL Data. We will create a single simple drive but you could create multiple drives and use storage spaces as an alternative. See Appendix Labs for details.

Perform the following tasks in the **Azure management portal**.

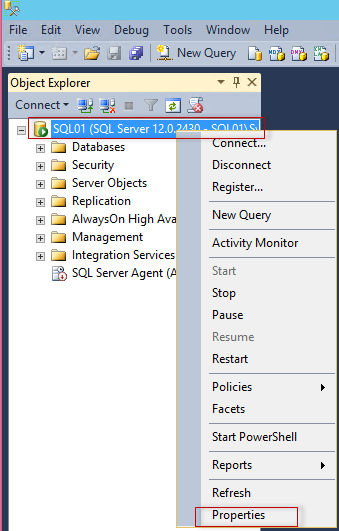
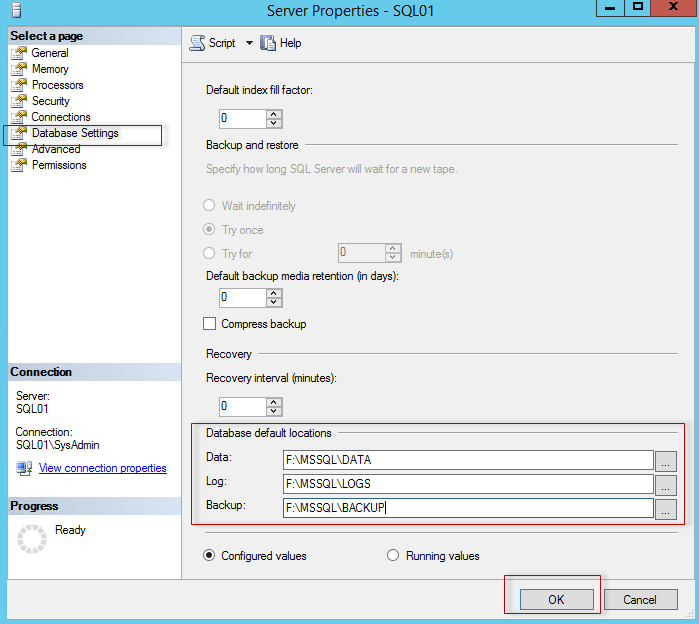
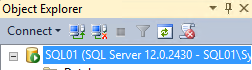
1. In the **Azure management portal**, click **VIRTUAL MACHINES**.
2. Click **SQL01**. Click **Dashboard**. On the virtual machine ***Dashboard*** page for ***SQL01***, click the **Attach** button (chain icon) located on the bottom navigation toolbar and select **Attach Empty Disk**.  Complete the following fields on the ***Attach an empty disk to the virtual machine*** form:   
       
   File Name: **sql01-sql01data**  
   Size**: 50 GB**   
   Host Cache Preference: **None**   
   
3. Click the Check Mark button to create and attach the new virtual hard disk to virtual machine.
4. On the virtual machine ***Dashboard*** page for **SQL01**, click the **Connect** button located on the **bottom toolbar** (far left icon) and click the **Open** button to launch a Remote Desktop Connection to the console of this virtual machine. Click Use another account to login at the console of your virtual machine with the local credentials defined above. Follow the prompts to continue connecting

|  |  |
| --- | --- |
| Property | Value |
| USER NAME | SysAdmin |
| NEW PASSWORD | Passw0rd! |

Perform the following tasks in an RDP connection to **SQL01**.

Now from the Remote Desktop console of *SQL01* we’ll create a new partition on the additional data disk attached above and format this partition as a new **F:** NTFSvolume. After formatting this new volume, you’ll create following folders:

* 1. F:\MSSQL
  2. F:\MSSQL\DATA
  3. F:\MSSQL\LOGS
  4. F:\MSSQL\BACKUP

1. Click **Yes** on the Networks Prompt to connect to other devices.
2. Once inside **Server Manager**, go to **Tools** (upper right corner menu) then select **Computer Management**.
3. Inside **Computer Management** select **Disk Management**. An “Initialize Disk” window will pop up, make sure the **new disk** is selected and click **OK**.
4. Right click unallocated space on **Disk 2** and select “**New Simple Volume…**” Click **Next**: then **Next** for the Specify Volume Size. The drive letter should be preconfigured to “**F**”, click **Next**:
5. Change the Volume Label to **DATA** and click **Next**: Click **Finish**.   
   **NOTE**: If you get a Microsoft Windows popup asking you if you want to format, you can just close it (we are already formatting the disk). Once you see the new F: drive in the upper volume window you can close the computer management window and continue.
6. Click on the **Folder** on the task bar to open **Computer**. Double-Click **Data (F:)** Click **Home** | **New Folder** type **MSSQL** press **Enter**. Press **Enter** again to drill down to the MSSQL folder then repeat the process to create the remaining folders (**DATA**; **LOGS**; **BACKUP**) You can then close the computer window and the Server Manager window to continue.
7. Open ***SQL Server Management Studio*** from the **Start Screen** and update default folder locations to the **F:** volume.   
   **Tip!** On the Windows **Start Screen**, you can quickly find the application tile for ***SQL Server Management Studio*** beginning to type the name of this application to automatically search for matching tiles.  
   1. Click **Start** – Type **SQL Server 2014 Management**
   2. Right Click **SQL Server 2014 Management Studio** and select “**Pin to Start**”
   3. Click **SQL Server 2014 Management Studio** on the start screen to launch the application. Connect to the SQL Server default instance using your Windows Account by clicking **Connect** on the **Connect to Server** window.
   4. Now, you will update the database’s default locations for DATA, LOGS and BACKUP folders. To do this, right click on your SQL Server instance Name **SQL01** (upper left corner) and select **Properties**.  
       
   5. Select **Database Settings** from the left side pane.
   6. Locate the **Database default locations** section and update the default values for each path to point to the new folder paths created above. Click OK  
      
   7. Right-Click **SQL01**  and select **Restart;** In the popup that asks **Are you Sure,** select **Yes.** if you go back into **properties**; you should see the change took place.  
      Close **SQL Server Management Studio**.

## Import and configure the testing database on SQL01

In this task, you will import the testing database provided by your development team. You will then create a user account that will be used by the web front end to access the data in the database.

Perform the following tasks in an RDP connection to **SQL01**.

1. First you will need to disable IE Enhanced Security mode.
2. Open **Server Manager**, and then select **Local Server**.
3. Click the hyperlink labeled **On** next to **IE Enhanced Security Configuration**.
4. In the dialog box, select **Off for Administrators**.
5. Click **OK**.
6. In **SQL01**, use **Internet Explorer** In the Security popup, select **Don’t use recommended settings** for now then click OK; Navigate to [**http://1drv.ms/1qFeJ2g**](http://1drv.ms/1qFeJ2g).
7. Right Click each of the **AdventureWorks** select **Download. Download**, **Save As** to store them in **F:\MSSQL\Data**.
   * You should have already created the F:\MSSQL\Data folder.
8. In **SQL01**, open **SQL Management Studio**.
9. Click **Connect**.
10. **In SQL Management Studio**, click **New Query (on the toolbar)**.
11. In the **Query Editor**, type the following query, and then press CTRL+E.(or click Execute button)

Create Database Test on (filename = 'F:\MSSQL\Data\adventureworks\_data.mdf'), (filename = 'F:\MSSQL\Data\adventureworks\_log.ldf') for attach

1. Expand **Databases**, and then verify you have a new database named **Test**. (If you do not see it, Right Click on **Databases**, select **Refresh**)
2. In **SQL Management Studio**, right-click **SQL01**, and then click **Properties**.
3. In **Server Properties**, click **Security**.
4. Under **Server authentication**, click **SQL Server and Windows Authentication mode**, and then click **OK**.
5. In the dialog box, click **OK**.
6. Right-click **SQL01**, and then click **Restart**.
7. In the dialog box, click **Yes**.
   * Wait for the restart to complete.
8. Under **SQL01**, expand **Security**, and then click **Logins**.
9. Right-click **Logins**, and then click **New Login**.
10. In **Login name**, type **DataManagementApp**.
11. Click **SQL Server authentication**.
12. In **Password** and **Confirm password**, type **Passw0rd!**
13. Uncheck **User must change password at next login**.
14. Click **User Mapping**.
15. Check the database **Test**, and then in the **Database role membership** area, check **DB\_datareader** and **DB\_Owner**.
16. Click Script at the top of the dialog to see what the Powershell would be to create the user and set permissions. It will be displayed in a tab behind the dialog.
17. Click **OK**.

## Configure firewall ports for SQL01

Next, you must enable WEBFE01and SQL01 to communicate internally within the service. While general IP connectivity is provided by DHCP, both servers are workgroup members and have the public firewall profile enabled. You will enable SQL Server traffic and PING traffic inbound on SQL01.

Perform the following tasks in an RDP connection to **SQL01**.

1. In your RDP session to **SQL01**, open **Server Manager**.
2. Click **Local Server**.
3. Next to **Windows Firewall**, click **Public: On**.
4. In **Windows Firewall**, click **Advanced settings**.
5. In **Windows Firewall with Advanced Security**, click **Inbound Rules**, and then click **New Rule**.
6. In **Rule Type**, click **Port**, and then click **Next**.
7. In **Specific local ports**, type **1433**, and then click **Next**.
8. On the **Action** page, click **Next**.
9. On the **Profile** page, click **Next**.
10. In **Name**, type **Allow SQL 1433**, and then click **Finish**.
11. In **Windows Firewall with Advanced Security**, click **Inbound Rules**, and then click **New Rule**.
12. In **Rule Type**, click **Custom**, and then click **Next**.
13. On the **Program** page, click **Next**. (All programs should be selected)
14. On the **Protocol and Ports** page, in Protocol type, select **ICMPv4**, and then click **Next**.
15. On the **Scope** page, click **Next**.
16. On the **Action** page, click **Next**.
17. On the **Profile** page, click **Next**.
18. In **Name**, type **PING**, and then click **Finish**.
19. Disconnect from the SQL01 RDP session.

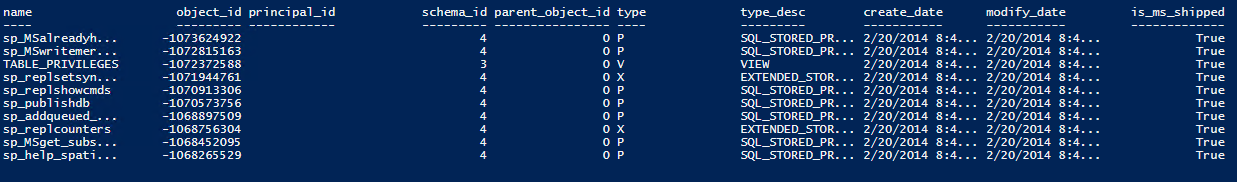
## Confirm Connectivity to SQL01 From WEBFE01

Next, let’s make sure we can successfully connect to **SQL01** from our Web Server.

Perform the following tasks in an RDP connection to **WEBFE01**

1. In the **Azure management portal**, click **VIRTUAL MACHINES**, click **WEBFE01**, and then click **Dashboard**.
2. On the bottom bar, click **CONNECT**, and then click **Open**.
3. Click **Connect**.
4. When prompted, log on as **sysadmin** using **Passw0rd!** as the password.
5. Click **yes**.
6. On **WEBFE01**, in Server Manager, Click **Local Server** – turn off IE Enhanced Security Configuration
7. On **WEBFE01**, in Server Manager, on the Tools menu, click **Windows PowerShell ISE**.
8. On the **View** menu, click **Show Scripting pane**.
9. In the **Command** pane, type **PING SQL01**, and then press **ENTER**.
   * The ping results indicate you can connect to SQL01 using the internal network provided by your service which contains the VMs.
10. Click on the **Folder** on the task bar to open **Computer**. Double-Click **Data (C:)** Click **Home** | **New Folder** type **AzureManagement** press **Enter** You can then close the computer window and the Server Manager window to continue.
11. Open a web browser Start – Internet Explorer. “Don’t use recommended settings” (for now) click OK
12. You need to **Add** the site **https://itcmaster.blob.core.windows.net** to your trusted sites. In **Internet Explorer** – Click **Tools** (Gear in upper right corner) – **Internet Options** – **Security** Tab – **Trusted Sites** – **Sites** – Type: **https://itcmaster.blob.core.windows.net** then click **Add** – **Close** - **OK**
13. **NOTE**: you can just click **OK** to any security warnings you get
14. Download **https://itcmaster.blob.core.windows.net/fy15q3/AzureManagement.zip** by typing the URL into the address bar on your **WEBFE01** server. Click Save as then save to **C:\AzureMangement** Folder   
    ***NOTE: The above URL is Case Sensitive!***
15. Using **File Explorer** Open the **c:\AzureManagement** folder, right-click on the **AzreManagement.zip** file; select **Extract All** Change the path to **C:\** then click **Extract**   
    Close “Local Disk (C:) window. You should have a window up still that is showing you **C:\AzureManagement\**
16. Open with **notepad** and copy the ***contents*** of the C**:\AzureManagement\Test Database Connectivity.txt** (**Test Database Connectivity)** file to your clipboard, and then on **WEBFE01**, in **Windows PowerShell ISE** paste in the Script pane.
17. ***NOTICE****: If you changed the computer name, username or password you will have to change the script to change the defaults at the top of the script*
18. Click the **play** button, or press **F5** to run the script.

The output of the script is a small set of system data which indicates you can communicate with the SQL Server instance on SQL01.



POWERSHELL Deep Dive:

All tasks performed on the SQL Server in this lab can be done using Powershell. If you want to see what it would look like check out: http://itproguru.com/downloads/SQLProvisionScript.txt

POWERSHELL Deep Dive:

To Add the Disk to the Azure VM you could run the command:

Set-AzureSubscription –SubscriptionName "<YourSubscriptionName>" -CurrentStorageAccount itcstoredan01

Get-AzureVM “ITCService<YourID>” -Name “SQL01” | Add-AzureDataDisk -CreateNew -DiskSizeInGB 50 -DiskLabel 'Data' -LUN 0 | Update-AzureVM

You do have to have the Azure Powershell Module installed and Powershell connected to your Azure Account (In Lab 5 we show you how ☺)

# Lab 5: Building Application Workloads – Deploy Data Access App

## Configure endpoints for WEBFE01

In this task, you will configure the required public endpoints for **WEBFE01**.

Perform the following tasks in the **Azure management portal**.

1. In the Azure management portal, click in **VIRTUAL MACHINES**.
2. Click **WEBFE01**, and then click **ENDPOINTS**.
3. Click **ADD**.
4. In **ADD ENDPOINT**, click the **Next** arrow.
5. In **Name**, select **HTTP**, and then click the **Completed** button.
6. Click **ADD**.
7. In **ADD ENDPOINT**, click the **Next** arrow.
8. In **Name**, select **HTTPS**, and then click the **Completed** button.
9. *You will have to wait for the endpoint to be created then continue*
10. Click **ADD**.
11. In **ADD ENDPOINT**, click the **Next** arrow.
12. In **NAME**, type **Custom5000**.
13. In **PUBLIC PORT** and **PRIVATE PORT**, type **5000**, and then click the **Completed** button.
14. Click **ADD**.
15. In **ADD ENDPOINT**, click the **Next** arrow.
16. In **NAME**, type **Custom5001**.
17. In **PUBLIC PORT** and **PRIVATE PORT**, type **5001**, and then click the **Completed** button.
18. Click **Dismiss Completed** in Azure Portal after all are done

## Configure firewall ports for WEBFE01

Next, you must enable WEBFE01 to communicate internally within the service. While general IP connectivity is provided by DHCP, both servers are workgroup members and have the public firewall profile enabled. You will enable Application ports and PING traffic on WEBFE01.

Perform the following tasks in an RDP connection to **WEBFE01**.

1. In your RDP session to **WEBFE01**, open **Server Manager**.
2. Click **Local Server**.
3. Next to **Windows Firewall**, click **Public: On**.
4. In **Windows Firewall**, click **Advanced settings**.
5. In **Windows Firewall with Advanced Security**, click **Inbound Rules**, and then click **New Rule**.
6. In **Rule Type**, click **Port**, and then click **Next**.
7. In **Specific local ports**, type **80, 443, 5000, 5001**, and then click **Next**.
8. On the **Action** page, click **Next**.
9. On the **Profile** page, click **Next**.
10. In **Name**, type **Allow WebApp**, and then click **Finish**.
11. In **Windows Firewall with Advanced Security**, click **Inbound Rules**, and then click **New Rule**.
12. In **Rule Type**, click **Custom**, and then click **Next**.
13. On the **Program** page, click **Next**. (All programs should be selected)
14. On the **Protocol and Ports** page, in Protocol type, select **ICMPv4**, and then click **Next**.
15. On the **Scope** page, click **Next**.
16. On the **Action** page, click **Next**.
17. On the **Profile** page, click **Next**.
18. In **Name**, type **Allow PING**, and then click **Finish**.
19. Disconnect from the RDP session.

## Remotely enable Internet Information Services on WEBFE01 using Windows PowerShell

In this task, you will use Windows PowerShell remoting to install Internet Information Services on WEBFE01. To perform this task, you will use standard Windows PowerShell remoting and administration commands; however, you must first install the Windows PowerShell remoting self-signed certificate installed in your WEBFE01VM. This is because Windows PowerShell remoting relies on HTTPS connections by default.

Perform the following tasks on your **SQL01** Server.

1. In the Azure management portal, click **VIRTUAL MACHINES**, click **SQL01**, and then click **Dashboard**. On the bottom bar, click **CONNECT**, and then click **Open**. Click **Connect**.
2. When prompted, log on as **sysadmin** using **Passw0rd!** as the password. Click **yes**.
3. Click on the **Folder** on the task bar to open **Computer**. Double-Click **Data (C:)** Click **Home** | **New Folder** type **AzureManagement** press **Enter.** You can then close the computer window and the **Server Manager** window to continue.
4. Open a web browser on **SQL01**.
5. You need to **Add** sites to your trusted sites.   
   **Start** – Click **Internet Explorer** – Click **Tools** (Gear in upper right corner) – **Internet Options** – **Security** Tab – **Trusted Sites** – **Sites** –   
   Type: **https://itcmaster.blob.core.windows.net** then click **Add**   
   Type: **https://manage.windowsazure.com** then click **Add**–**Close** - **OK**
6. Download and Extract **https://itcmaster.blob.core.windows.net/fy15q3/AzureManagement.zip** to your **SQL01** server in the **C:\AzureMangement** Folder   
   ***NOTE: The above URL is Case Sensitive!***
7. **NOTE**: you can just click OK to any security warnings you get
8. Download **https://itcmaster.blob.core.windows.net/fy15q3/AzureManagement.zip** by typing the URL into the address bar on your **SQL01** server. Click Save as then save to **C:\AzureMangement** Folder
9. Using **File Explorer** open the **c:\AzureManagement** folder, right-click on the **AzureManagement.zip** file; select **Extract All**. Change the path to **C:\** then click **Extract**. Close “Local Disk (C:) window. You should have a window up still that is showing you **C:\AzureManagement\**
10. On **SQL01**, in **Server Manager**, on the **Tools** menu, click **Windows PowerShell ISE**.On the View menu, click **Show Scripting pane**.
11. On your **SQL01** server, run the **C:\AzureManagement\WindowsAzurePowerShell.3f.3f.3fnew.exe** file to install Azure Powershell Extentions
    * Click **Install**
    * Click **I Accept**
    * Click **Finish**
    * Click **Exit**
12. Open **Windows PowerShell ISE** as **Administrator**. (Start – Type **PowerShell ISE**, Right-Click **Windows PowerShell ISE** – Click **Run as Administrator**)
13. We now need to enable Azure PowerShell commands by clicking the run pane (bottom) type the “Import-Module Azure” command then press <ENTER>

**Import-Module Azure**

1. From the menu choose **File** **Open** to open the script file **C:\AzureManagement\Remote PowerShell Script Configuration.ps1**.
2. Highlight the script under **Part 1**, and then press **F8**.
3. In the presented web page, log on using your Microsoft Azure account, and then download the **PublishSettings** file that is presented.
4. Save the **PublishSettings** file in the **C:\AzureManagement\** folder on the computer.
5. In the script file, in part 2, replace the text **##Your Script File Path Here##** with the full path to your downloaded file, such as **“C:\AzureManagement\Free Trial-6-4-2014-credentials.publishsettings”**.  
   **NOTE**: If there are spaces in your file name, you will have to wrap the path and filename in quotes (“) as shown in the example
6. Highlight the script under **Part 2**, and then press **F8**.
   * You should see basic information on your subscription in the output.
7. Highlight the script under **Part 3**, and then press **F8**. When prompted, type your **unique ID**.
   * You will now have installed the certificate used by the WEBFE01 VM, which will enable remote Windows PowerShell access.
8. In **Windows PowerShell**, type the following command, and then press **ENTER**. Replace **<ID>** with your unique identifier.

**Get-AzureVM –Name WEBFE01 –ServiceName ITCService<ID> | Get-AzureEndPoint | Select Name, Port | FT –AutoSize**

1. You are now presented with a list of ports that are open on **WEBFE01**. Using the output of the command above, identify the port used for Windows PowerShell.
2. In **Windows PowerShell** (or in the PowerShell window of **ISE**), type the following command, and then press **ENTER**. Replace **<ID>** with your unique identifier. Replace **<PORT>** with the Windows PowerShell port from the previous command output.

**Enter-PSSession –ComputerName ITCService<ID>.cloudapp.net –Port <PORT> -Credential sysadmin –UseSSL**

1. In the **Password** dialog box, type **Passw0rd!**, and then click **OK**. Note: if you changed the username and password when you created the machine, you will have to use the username and password you used to create the machine.
2. In **Windows PowerShell**, type **Hostname**, and then press **ENTER**.
   * You are now in a Windows PowerShell session on your Azure WEBFE01 VM from SQL01.
3. In **Windows PowerShell**, type the following command, and then press ENTER. This will install a full IIS server.

**Get-WindowsFeature Web-Server | Add-WindowsFeature –IncludeAllSubfeature**

* + Wait for the command to complete before proceeding. BE PATIENT. It takes several minutes.

1. In **Windows PowerShell**, type the following command, and then press ENTER. This will restart IIS

**Iisreset**

* + Wait for the command to complete before proceeding.

1. On your Local Laptop, using **Internet Explorer**, navigate to **http://itcservice<ID>.cloudapp.net** where **<ID>** is your unique identifier.
   * You have now connected to your running web server and are ready to hand off this environment for installation of your company’s software.
   * If you cannot connect, wait 2 mins and try the IISReset again. if that still does not work, check to make sure your firewall parts and endpoints were not skipped or botched.

## Deploy and test the Contoso Data Access sample site

In this task, you will deploy a sample site. The sample web site simulates the types of tasks the Contoso production application performs, and will prove that the Azure infrastructure meets the base technical requirements of the production system.

Perform the following tasks in RDP sessions to **WEBFE01**.

1. Switch to the RDP session for **WEBFE01**.
2. Using **File Explorer**, navigate to **c:\inetpub\wwwroot**.
3. Delete all files and folders in this folder.
4. Using **File Explorer**, navigate to Navigate to **C:\AzureMangement\Website**.
5. Copy all Files and folders from **C:\AzureMangement\Website\**[Website] to **C:\inetpub\wwwroot**.
   * The global.asax file should be directly in the C:\inetpub\wwwroot folder, not a subfolder.
6. Open the **Web.Config** file in **Notepad**, and then locate the following lines.
   * This connection string provided by the developer of the application assumes a locally installed SQL database, and assumes the locally logged on user has permission to access the database. This is not appropriate for a distributed web application and you will be updating the database location, name, and the credentials used.

<connectionStrings>

<add name="AdventureWorksConnection" connectionString="data source=.\MSSQL14;initial catalog=AdventureWorks;***integrated security=True***; multipleactiveresultsets=True;application name=EntityFramework" providerName="System.Data.SqlClient" />

</connectionStrings>

1. Edit the line so that it reads as follows. Changed information is highlighted in yellow, new information is highlighted in green, and removed information is highlighted in red (in above).
   * This configures the sample application to use the database stored on SQL01 named Test. There are three changes that are made. You change the SQL Server Name (data source), you change the database name (initial catalog), and you replace the credential with a fixed username and password (integrated security replaced with user and password) If you changed your password for DataManagementApp SQL user you will need to change it here too.
   * You can optionally, copy the following XML from this document to web server's web.config file. Note that there should only be three lines in the final file for <connectionStrings> the open (<conn…), <add name…, and close (</conn…)

<connectionStrings>

<add name="AdventureWorksConnection" connectionString="***data source=SQL01***;initial catalog=***test;user id=DataManagementApp;  
password=Passw0rd!;***multipleactiveresultsets=True;application name=EntityFramework" providerName="System.Data.SqlClient" />

</connectionStrings>

1. On your **Local** Laptop computer, using **Internet Explorer**, navigate to **http://itcservice<id>.cloudapp.net**.  
   **NOTE**: You may have to refresh your browser.
2. Under **Data Management Login**, type **12345**, and then click **Login**.
3. Click **Product Listings**.
   * The result set indicates the web application is communicating with the hosted SQL database correctly.



# Lab 6 Create a new Ubuntu Linux VM using the gallery

In this task, you will create a new Ubuntu Linux VM, and then configure it to be managed via Remote Desktop. The remote desktop phase will take some time, so you will verify it later.

Perform the following tasks in the Azure management portal.

1. In the Azure management portal, click **NEW**.
2. Click **COMPUTE**, click **VIRTUAL MACHINE**, and then click **FROM GALLERY**.
3. In **Choose an Image**, click **UBUNTU**, click **Ubuntu Server 14.04 LTS**, and then click the **Next** arrow.
4. Create a new virtual machine using the values in the following table, and then click the Next arrow.

|  |  |
| --- | --- |
| **Property** | **Value** |
| DNS NAME | **Linux01** |
| TIER | **Standard** |
| SIZE | **A3** |
| USER NAME | **AzureUser** |
| AUTHENTICATION | **Select only PROVIDE A PASSWORD** |
| NEW PASSWORD and CONFIRM | **Passw0rd!** |

1. On the Virtual machine configuration page, in **CLOUD SERVICE**, select **itcservice<ID>**.
2. In **STORAGE ACCOUNT** select **itsstore<ID>**.
3. In **ENDPOINTS**, in **ENTER OR SELECT A VALUE**, select **REMOTE DESKTOP**, and then click the **Next** arrow.
4. Click the **Complete** icon.
   1. The virtual machine will take a few minutes to create. Depending on the load this may take between 5 and 25 minutes.
   2. Wait for the new virtual machine to finish before proceeding.

## Connect to the new Linux VM using SSH and RDP

In this task, you will use a Secure Shell (SSH) connection to manage **Linux01** and install both the desktop and RDP protocol server. This step can take upwards of 30 minutes due to installation times. You can choose to wait, or start the installation, move on, and then complete this step at a later time.

Perform the following tasks on your admin workstation.

1. On your local workstation you’ll need some files from our AzureManagement.zip file.
   1. Using **Internet Explorer**, download and extract **https://itcmaster.blob.core.windows.net/fy15q3/AzureManagement.zip** to your create an **\AzureManagement** folder (either at the root of C:\, or on your desktop).
      1. NOTE: The above URL is Case Sensitive!
2. In **\AzureManagement**, double-click **PuTTY.exe**.
3. In **Host Name (or IP address)**, type **ITCService<ID>.cloudapp.net**, and then click **Open**.
   1. <ID> is your unique id.
4. In the **PuTTY Security Alert** dialog box, click **Yes**.
5. Log on as **AzureUser** using **Passw0rd!** as the password.
   1. You are low logged on to your new Linux VM using SSH.
6. Type the following commands, pressing **ENTER** after each one. This set of commands will add a desktop and enable RDP. Confirm each command as needed.

**sudo apt-get update**

**sudo apt-get install Ubuntu-desktop**

* 1. Enter **Y** when prompted.
  2. This process will take up to 30 minutes or longer. You can allow this to run in the background and come back later. This VM will not be used again for other labs.

**sudo apt-get install xrdp**

**sudo /etc/init.d/xrdp start**

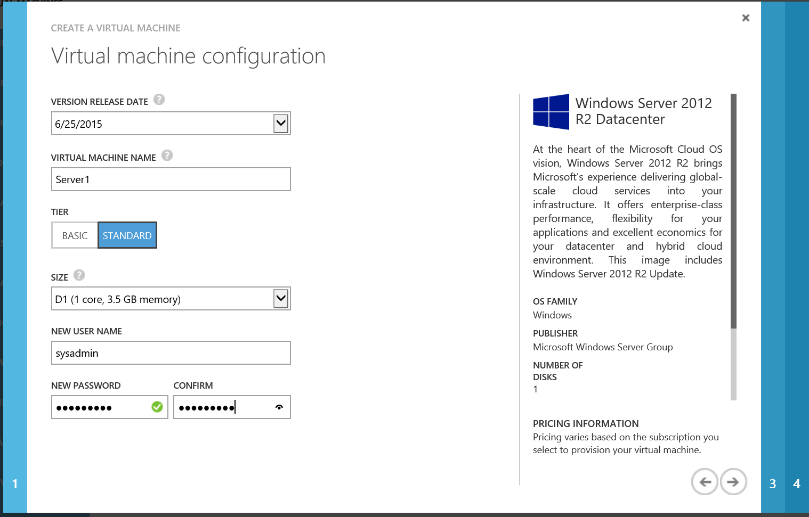
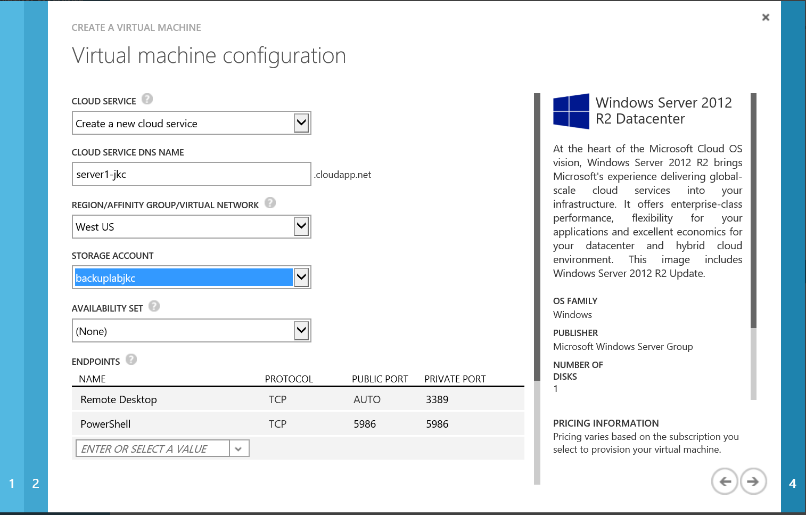
* 1. This last command ensures the xRPD server is started, as it does not always automatically start.

1. Now you should be able to go back to the Azure portal, select your **Linux01** virtual machine, and **connect** to it using RDP.

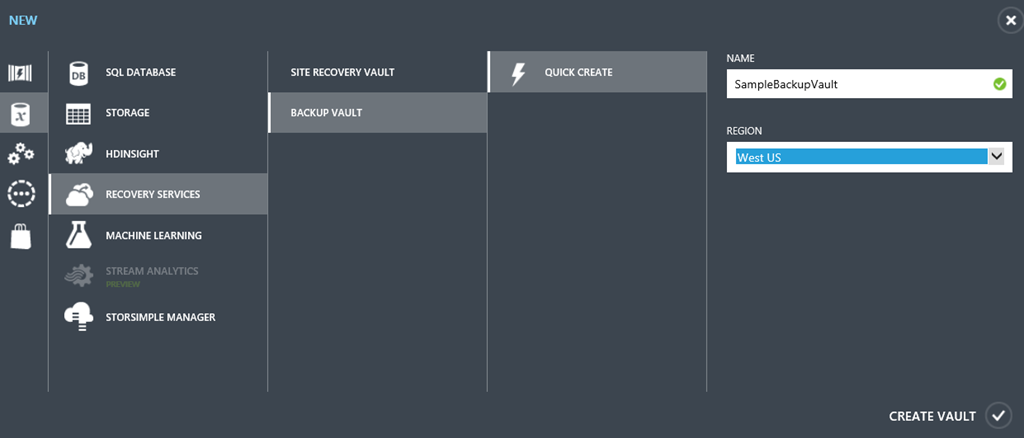
# Lab 7 - Backup an Azure VM

In this lab, you will use the Azure Portal to backup an Azure Virtual Machine.

#### Create a new Storage Group and Virtual Machine

1. Log into the Azure Portal at <http://manage.windowsazure.com>
2. On the lower left, select “NEW”
3. Select **DATA SERVICES -> STORAGE -> QUICK CREATE**
4. For the Storage Account Configuration, use:
   1. URL – **backuplab<unique>** Use “backuplab” and something unique to you to complete the FQDN.
   2. Location – **West US** (You are welcome to use any location, just use that same region throughout all the labs for consistency.)
   3. Replication - **Locally Redundant**
5. Select **COMPUTE -> VIRTUAL MACHINE -> FROM GALLERY**
6. For Image, select   
   **Windows Server 2012 R2 Datacenter**
7. For Virtual Machine Configuration, use:
   1. Version Release Date - <most recent date>
   2. Virtual Machine Name – SERVER1
   3. Tier – Standard
   4. Size – A1
   5. Username – **sysadmin**
   6. Password – **Passw0rd!**
8. For the second configuration page, use:
   1. Cloud Service – Create New
   2. Cloud Service Name – <must be unique for you>
   3. Region – **West US**
   4. Storage Account - <Select the account your created in Step #4
   5. Availability Set – None
   6. Endpoints – Leave as default
9. Leave the final page of the configuration wizard at its defaults and click the checkmark at the bottom right to create the virtual machine. (It will take a few minutes to configure the virtual machine, continue on in the lab.)

## Create a Backup Vault

1. On the lower left, select **“NEW”**
2. Select **DATA SERVICES -> RECOVERY SERVICES -> BACKUP VAULT -> QUICK CREATE**
3. For the Vault Configuration, use:
   1. Name – **“BackupLabVault”**
   2. Region – **West US**

#### Protect a Virtual Machine

Wait for your virtual machine status to become “running” before continuing with the lab steps.

1. Go to "Recovery Services" on the left hand scroll bar. Click on your backup vault and you will be on the quick start page indicating that your vault was created. Click the **“Registered Items”** tab at the top. You will have no items registered.
2. Click the **“Discover”** icon in the bottom navigation bar.
3. Once the discover process completes, click “**Register”** to access a list of Azure Virtual Machines. Check the box next to your server, then click the checkmark at the bottom right of wizard to continue. Wait for the status of your VM to become “**Registered**”.
4. Click the **Policies** tab.
5. Review the “DefaultPolicy” and edit it to perform the backup as soon as possible. Backups can be scheduled on any half hour segment. Set the backup time to be the next closest ½ hour mark.  (You will have to de-select the already-checked time before selecting your new backup time.) Save your changes.
6. Click on the “Recovery Services” tab on the far left of the Azure portal. Then click on the name of the backup vault you just created. Confirm that you are on the “quick launch” page (denoted by a cloud in the navigation bar) and scroll all the way to the bottom of the page. Under Protect Azure Virtual Machines choose the “Protect Virtual Machines” link under number 3. 
7. Click **“Protect”** from the bottom navigation bar.Select your server from the list of registered servers. Configure protection using the DefaultPolicy that you edited.  
   
8. The backup job with take about 15 minutes and may start a few minutes after your selected time. Wait until the backup job is completed. You can check the status of the jobs using the **Jobs** tab.

## Restore a Virtual Machine

1. From your list of Virtual Machines, delete your Server-1. Do not retain the disks.
2. Go to **RECOVERY SERVICES** and select your backup vault.
3. Go to the **Protected Items** tab.
4. Highlight your server name and you should have one recovery point. Select **Restore** from the bottom navigation.
5. Step through the wizard to select the recovery point (you will only have one option) and kick off the restoration. It will take about 20 minutes for the server to be recovered.

# Lab 8 – Using Azure Backup

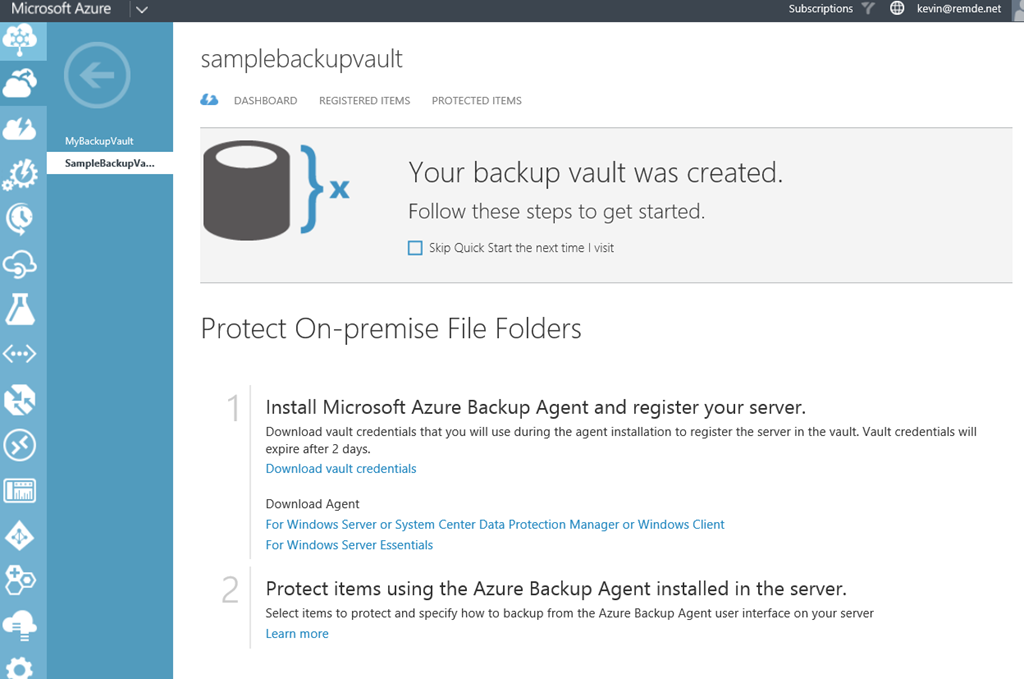
In this lab, you will simulate using Azure as a backup destination for a Windows Server or client device you have on-prem. To avoid installing the backup client on your local workstation, you will build a Windows Server in Azure to use as the source machine.

#### Create a Virtual Machine as your Source Server

1. Go to **COMPUTE -> VIRTUAL MACHINE -> QUICK CREATE.** Enter a unique name for your server (such as SERVER02 and add something unique like your initials to this server name), select the same region you used in Lab 1 and set a username and password. We recommend sysadmin/Passw0rd!

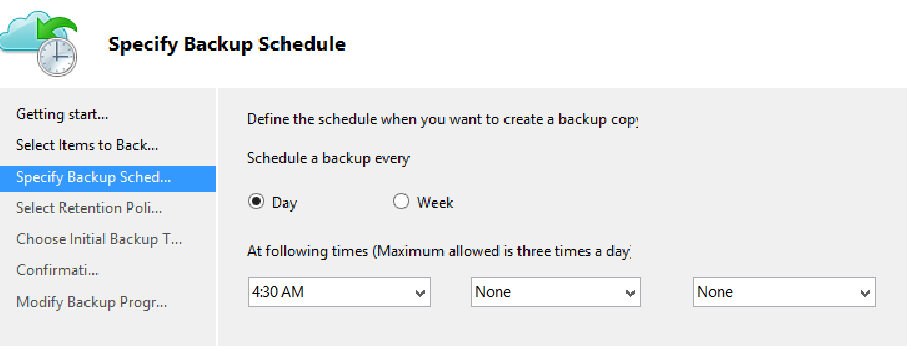
#### Establish a Trust to Azure

To establish a secure trust between your backup vault and the server being backed up, you will need to download the vault credentials. These credentials will be used to initially register a server or workstation or to recover items to a new machine. Because you will need to install these credentials directly on the machine, log into your newly created VM.

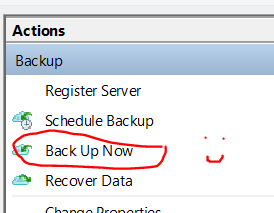
1. Once it is in a running state, select your newly created virtual machine. Click **Connect** from the bottom navigation bar and log into it via RDP.
2. Server Manager should launch automatically. Select **Local Server** and turn off IE’s Enhanced Security mode.
3. Launch File Explorer and create the C:\Important\_Stuff folder on your server. Inside that folder, create a blank txt file or other document called “This Is Very Important.txt” (You will be backing up this folder later in the lab.)
4. While still on the RDP Console of Server2, click on the Windows button in the bottom left hand of the screen and launch Internet Explorer. Navigate to <http://manage.windowsazure.com>. Log into your Azure Subscription.
5. On the left-hand navigation, scroll to **RECOVERY SERVICES.**
6. Click the name of the backup vault you created in Lab 1 to get to the Quick Start page. Click **Download Credentials**. Save the file some you’ll remember on the machine to be backed up. *In a production environment, you’ll want to treat these credential files with care.*
7. Return to the Quick Start page and download the backup agent for **Windows Server or System Center Data Protection Manager or Windows Client** and run it to install.
8. For the purposes of the lab, you can accept all the defaults. The agent will install any other missing required components. Select "I do not want to use Microsoft Updates" for this lab exercise.
9. If the client software does not automatically launch, click on the Windows button, go to Start, type in Azure, then click on Microsoft Azure Backup. In the right hand menu action pane click on **Register Server** in order to associate your server with your Azure subscription.
10. When prompted, browse to the location you saved your vault credentials and then click **Next.**
11. On the **Encryption Settings** page, you can either generate or enter your own Passphrase. Enter a local drive to save the passphrase file for this lab, however in production these passphrases should be kept somewhere secure.
12. Click “Finish” to complete the registration process.
13. Once finished with registration click “Close”. This will return you to the Microsoft Azure Backup client software.

#### Configure the Back Up Job

At this point, you have done all the configuration of your server to backup data to Azure. If you return to the Backup Vault configuration in the Azure portal, you will see the name of the server listed in the “protected” tab. In the next steps, you’ll configure your backup job.

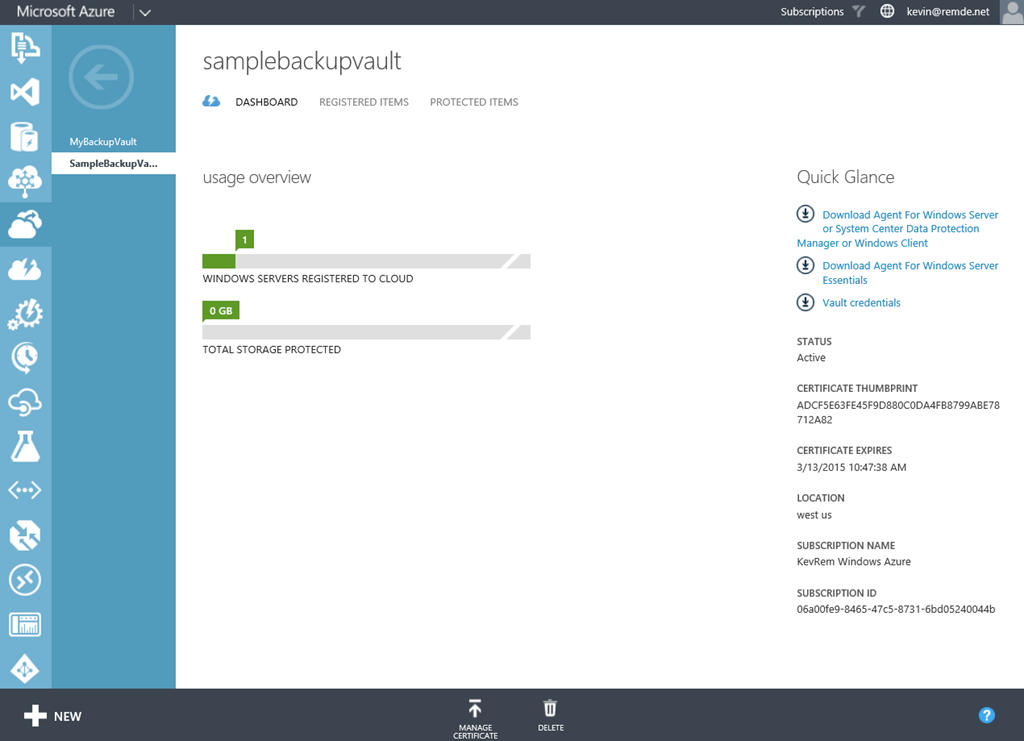
1. In the Microsoft Azure Backup tool, in the Actions pane, click on “Schedule Backup”.
2. Click “Next” on the Getting Started page to move onto the “Select Items to Backup” portion of the wizard.
3. Browse to and select the “C:\Important\_Stuff” folder you created earlier. Click “Next”.
4. On the “Specify Backup Schedule” page notice that you can choose to backup daily at a certain time, or during specific days of the week. Scheduled your backup for daily at 4:30am, then click “next”. 
5. On the “Select Retention Policy” page, review the options for retaining the backed-up data. You do not need to make any adjustments for lab. Accept the defaults and click “next”.
6. On the “Choose Initial Backup Type”, use the **"Automatically over the network"** default setting. You do have the option to “seed” your backup in an “offline” way as well.
7. On the “Confirmation” page, review your selections and click “Finish” to create the backup schedule.

No backup has launched yet, but would happen based on the schedule you’ve set.

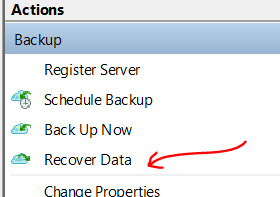
1. Click the **“Back Up Now”** option in the Actions pane.
2. On the resulting **Confirmation** page, click **“Back Up”.** Leave the console open to watch the status of this small backup job until it is completed. For larger jobs, you can close the status window and let the launched job run in the background.
3. Delete the file "This Is Very Important.txt" from your server. We will now verify the backup and restore the file.

#### Verify the Data in the Backup Vault

To confirm that the backup was successful, review the status of the Backup Vault in Azure.

1. Return to the Azure Portal and navigate to the **RECOVERY SERVICES** section. Click on the Backup Vault.
2. Select the **Dashboard** tab, you will see that you have one server registered with 0 GB protected. (The small size of the file backed up doesn’t register in the portal dashboard.)
3. Select the **Registered Items** tab, notice that Azure Virtual Machine is still listed from the previous lab. Drop down the menu and select “Windows Server” then click on the checkmark to the right to see the newly added on-prem server listed. This is where you can delete registrations of decommissioned servers as well.
4. Select the **Protected Items** tab. Here you can see some basic information about what is protected. A file folder with only one recovery point available.

#### Restore Deleted Data

1. On your Source Server, minimize the Azure Portal window and launch File Explorer. Delete the file you created in your C:\Important\_Stuff folder.
2. Return to the Microsoft Azure Backup console and click “Recover Data” in the Action pane.
3. On the **Getting Started** page, select “This server”, since the machine was the original backup source and is already registered with the backup vault. If you were on a new machine, you would be prompted to provide the vault credentials before continuing.
4. On the **Select Recovery Mode** page, select “Browse for files” and click “next”.
5. On the **Select Volume and Date** page, use the drop down menu to pick the volume and date available. You will only have one option since you only have one recovery point at this time.
6. On the **Select Items to Recover** page, browse to the file that was deleted, select it and click “next”.
7. On the **Specify Recovery Options** page, review the options to recover to a different location, duplication handling and permissions management. For this lab, leave the defaults and click “next.”
8. On the **Confirmation** page, click “recover” and close the window.
9. Back in the Microsoft Azure Backup console, you can see the recovery job status.
10. Once completed, browse to the file location on the server and verify it was restored.

# Lab 9 – Copy Files with AZCopy

AZCopy is a useful command line tool for copying files with the Azure Cloud Storage. You can use it to copy files up to Azure Storage for backup purposes. You can use it to copy files from one Azure Storage Account to another Azure Storage Account and it will perform a server to server copy. We will cover two scenarios in this lab.

Scenario 1:   
In the first part of this lab you will use the command line tool called AZCopy to recursively copy a subdirectory and files from your local machine to Azure Storage.

Scenario 2:   
In the second part of this lab you will use AZCopy to copy a VHD from one storage account to another.

## Install AZCopy on your Local Machine

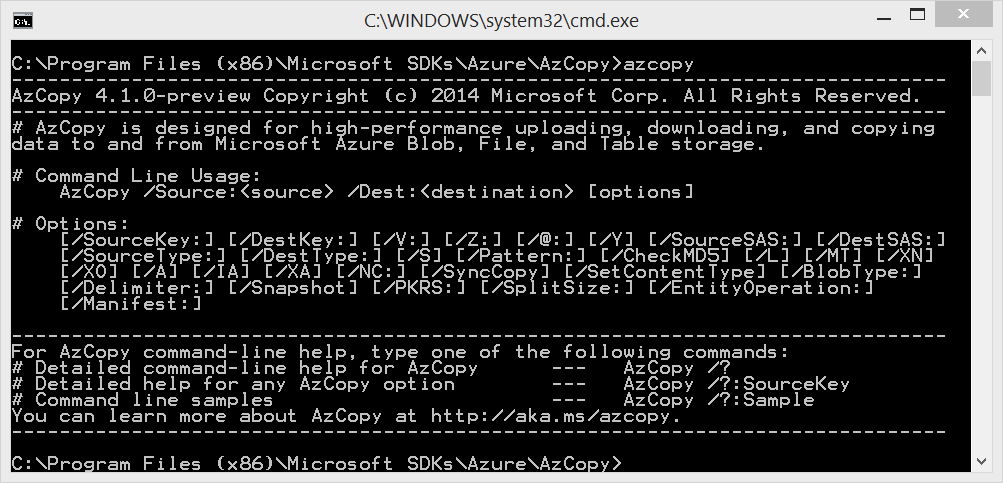
1. Download the AZCopy tool (http://aka.ms/downloadazcopy) and install it on your local machine.
2. Open a command prompt and change to the directory where AZCopy is installed.  
   (By default, the AzCopy installation creates a folder named AzCopy under %ProgramFiles(x86)%\Microsoft SDKs\Azure\ (on 64-bit Windows) or %ProgramFiles%\Microsoft SDKs\Azure\ (on 32-bit Windows).)

At the command prompt enter the following command:

cd "\Program Files (x86)\Microsoft SDKs\Azure\AzCopy"

Press Enter.

1. Type azcopy.exe [enter]  
   You should see this:



## Locating storage access key; Preparing to copy files

1. Click the Windows button and type in Notepad, then launch Notepad.exe (We will use notepad to keep track of your information and build your commands)
2. Head back to the Azure Management Portal, click on Storage in the left navigation menu, locate the storage account you created in Lab 1. At the **Dashboard** tab, look in the navigation bar at the bottom, click **Manage Access Keys.** Copy your primary key to notepad.
3. On the **Dashboard** tab of your storage account, copy the blob endpoint URL and paste it into notepad. It will be something similar to: *https://<storageaccountname>.blob.core.windows.net or https://*backuplab<unique>*.blob.core.windows.net*
4. Create a folder named “myfolder” on your c: drive. “C:\myfolder”

Copy the "This Is Very Important.txt" into the new folder named c:\myfolder.

## Upload files from the file system to Blob storage

Due to the time needed to upload a full VHD over shared Wi-Fi, these next steps are demonstrated with basic text files. However, you could use a similar process to upload a VHDs from your local network to Azure.

Using notepad file as a scratch area, build the command for copying your Lab Notes to Azure. In the command below, indicate the source location of your notes file, the correct account name for your storage account, the key for access to your storage account and the proper name of your notes file.  
  
AzCopy /Source:C:\myfolder /Dest:<storage URL>/labfiles /DestKey:key /Pattern: "This Is Very Important.txt"

It will look something similar to this:

|  |
| --- |
| AzCopy /Source:C:\myfolder /Dest:https:// backuplab<unique>.blob.core.windows.net/mycontainer /DestKey:<insert that long key you copied to notepad here> /S /Pattern:\*.txt |

Specifying option /S copies the contents of the specified directory to Blob storage recursively, meaning that all subfolders and their files will be copied as well.

1. Using CTRL-C or right click and “copy” to copy your command from notepad and right click paste to insert the command into your AZCopy window to execute.
2. Once the command completes, you can verify the addition of the containers and the files to your azure storage account by using the Azure portal. Click on the Storage tab, click on your Storage Account, click on the containers tab at the top, lastly browse to your folder or file.

#### Copy a VHD Blob between Storage Accounts

Extra Credit

|  |
| --- |
| As an extra credit exercise work with someone else near you to copy a vhd file from their storage account to your storage account and then import the VHD in as a VM. This is similar to the exercise below but you would use their storage account instead of itcampdata.blob.core.windows.net where we have a vhd for you to copy. There are several ways you can accomplish this including creating a publicly accessible folder or sharing keys. Have fun! |

We placed a VHD file located on an Azure Storage Account that we gave public read access to. This is just an Azure Storage area that has a backup of a VM. You will copy down this VHD file and then build an Azure VM using this VHD disk.

The file is named “WinITcamp-WinITcamp-2015-08-04.vhd” and is located in the “https://itcampdata.blob.core.windows.net/” storage account in a container called “bkup”

Here is the full link:

https://itcampdata.blob.core.windows.net/bkup/WinITcamp-WinITcamp-2015-08-04.vhd

1. Using your notepad file as a scratch area, build the command for copying a VHD blob between storage accounts in Azure. In the command below, indicate the source location of your VHD, the correct accounts name for your storage accounts, the keys for access to your storage accounts. This copy will complete in seconds if within the West US region or about 10-15 minutes to run across US regions.

AzCopy /Source:<storageaccount1 URL>/vhds /Dest:<storageaccount2 URL>/vhds /SourceKey:your-key /DestKey:your-key2 /S

Your command will look similar to this:

|  |
| --- |
| AzCopy /Source:https://itcampdata.blob.core.windows.net/bkup /Dest:https:// backuplab<unique>.blob.core.windows.net/mycontainer /DestKey:<insert your key> /Pattern:WinITcamp-WinITcamp-2015-08-04.vhd /S |

1. Using CTRL-C or right click and “copy” to copy your command from notepad and right click paste to insert the command into your AZCopy window to execute.
2. Once the command completes, you can verify the addition of the VHD to your storage account.

#### Create an VM from your copied disk

1. In the Azure portal, go to the **VIRTUAL MACHINE** section. Click the **DISKS** tab. In this list, you will see all the disks recognized as server VHDs files. At the bottom, click **CREATE.**
2. Enter a reference name for your new disk, such as **Server1-copy**. (This will not change the name of the actual file in the storage account.)
3. Enter the URL for the file you copied to the new storage account.
4. Select the checkbox to indicate that the VHD contains an operating system.
5. Select “Windows” from the Operating System Family. Click the circled checkbox to finish the operation.
6. Select **+NEW** from the bottom right of the Azure Portal to create a new Virtual Machine.
7. Select **COMPUTE -> VIRTUAL MACHINE -> FROM GALLERY**
8. Do not select an operating system image, instead highlight “My Disks” from the bottom left navigation in the wizard. Your newly created disk should be available to select.
9. Give the new virtual machine a name like “**WinITcamp”** and select D1 for the size.
10. For the Cloud Service name page:
    1. Cloud Service – Create New
    2. Cloud Service Name – <must be unique for you>
    3. Region – **West US**
    4. Storage Account - <Select the account where your new copy resides>
    5. Availability Set – None
11. Endpoints – Leave as default
12. Click through the remaining screen without any changes and complete the wizard.
13. Once the machine is running, you can connect via RDP using the same username and password as the original server (sysadmin/Passw0rd!)

AZCopy has more to offer and if you are interested in all it can do for you, take a look at the Azure team blog article here: <https://azure.microsoft.com/en-us/documentation/articles/storage-use-azcopy/>

# Lab 10 - Backing up a Windows Client to Microsoft Azure Recovery Services Backup Vault

To back up files and data from your Windows Clients, Windows Server or System Center Data Protection Manager (SCDPM) to Azure or when backing up IaaS VMs to Azure, you must create a backup vault in the geographic region where you want to store the data. In this lab, we are going to backup a Windows Client machine to Microsoft Azure. Your machine can be Windows 7, Windows 8, Windows 8.1 or Windows 10. Make sure you have the latest service packs on your machine as well. Backups to a vault can be up to 1.7 Terabytes in size.

For more information on Microsoft Azure Recovery Services Backup Vault go to: <http://azure.microsoft.com/en-us/services/backup> For FAQ’s on Microsoft Azure Backup go to: [https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq](https://manage.windowsazure.com/)

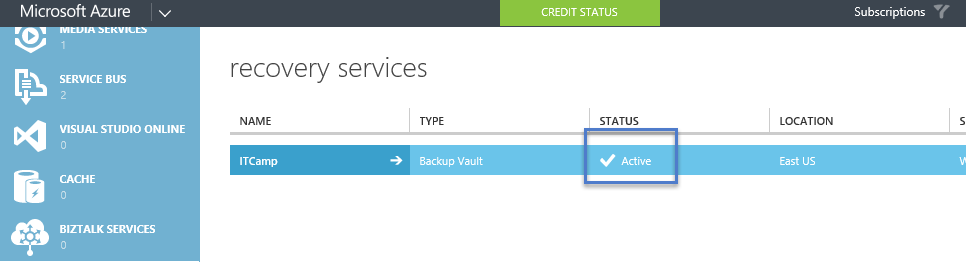
## Create a Backup Vault

1. Sign in to the Management Portal <https://manage.windowsazure.com>
2. Click **New** -> **Data Services** -> **Recovery Services** -> **Backup Vault** and choose **Quick Create**

* For the **Name** parameter, enter a friendly name to identify the backup vault. This needs to be unique for each subscription.
* For the **Region** parameter, select the geographic region for the backup vault. The choice determines the geo to which your backup data is sent. By choosing a geo close to your location, you can reduce the network latency when backing up to Azure.
* Click **Create Vault** to complete the workflow. It can take a while for the backup vault to be created. To check the status, you can monitor the notifications at the bottom of the portal.



1. After the backup vault has been created, a message will tell you the vault has been successfully created and it will be listed in the resources for Recovery Services as **Active**.



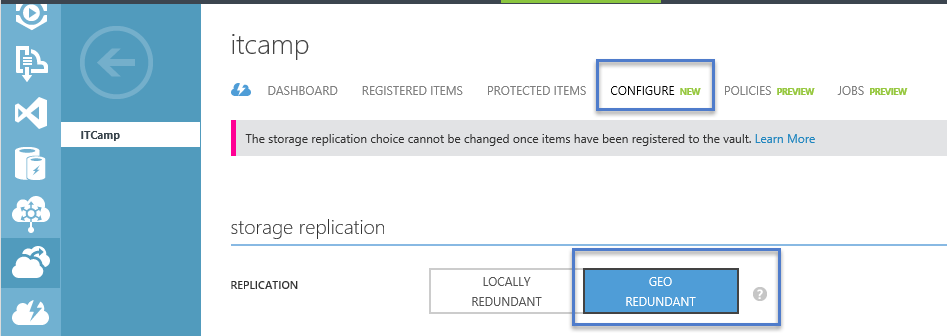
#### Azure Backup - Storage Redundancy Options

The best time to identify your storage redundancy option is right after vault creation, and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.

Your business needs would determine the storage redundancy of the Azure Backup backend storage. If you are using Azure as a primary backup storage endpoint (e.g. you are backing up to Azure from a Windows Server), you should consider picking (the default) Geo-Redundant storage option. This is seen under the **Configure** option of your Backup vault.

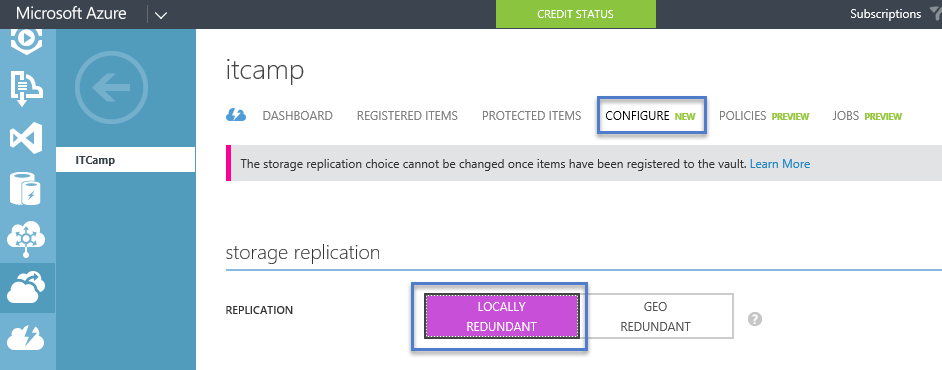
#### Geo-Redundant Storage (GRS)

GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region, and is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, by storing data in GRS, Azure Backup ensures that your data is durable in two separate regions.



#### Locally Redundant Storage (LRS)

Locally redundant storage (LRS) maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from the failure of an entire Azure facility.

If you are using Azure as a tertiary backup storage endpoint (e.g. you are using SCDPM to have a local backup copy on-premises & using Azure for your long term retention needs), you should consider choosing Locally Redundant Storage from the **Configure** option of your Backup vault. This brings down the cost of storing data in Azure, while providing a lower level of durability for your data that might be acceptable for tertiary copies.

#### Note

* As of March 2015, customers do not have a programmatic (eg: PowerShell) way of creating a backup vault.
* The storage redundancy should be selected right after vault creation, and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.

#### Download Vault Credentials

Using vault credentials to authenticate with the Azure Backup service.

The on-premises server (Windows client or Windows Server or SCDPM server) needs to be authenticated with a backup vault before it can back up data to Azure. The authentication is achieved using “vault credentials”. The concept of vault credentials is similar to the concept of a “publish settings” file which is used in Azure PowerShell.

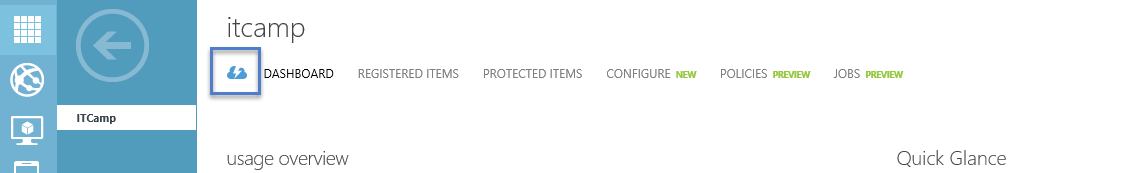
#### What is the vault credential file?

The vault credentials file is a certificate which is generated by the portal for each backup vault. The portal then uploads the public key to the Access Control Service (or ACS). The private key of the certificate is made available to the user as part of the workflow which is given as an input in the machine registration workflow. This authenticates the machine to send backup data to an identified vault in the Azure Backup service. It is worth calling out that the vault credential is used only during the registration workflow. It is the user’s responsibility to ensure that the vault credentials file is not compromised. If it falls in the hands of any rogue-user, the vault credentials file can be used to register other machines against the same vault. However, as the backup data is encrypted using a passphrase which belongs to the customer, existing backup data cannot be compromised. To mitigate this concern, the vault credentials is set of expire in 48hrs. You can download the vault credentials of a backup vault any number of times – but only the latest vault credential file is applicable during the registration workflow.

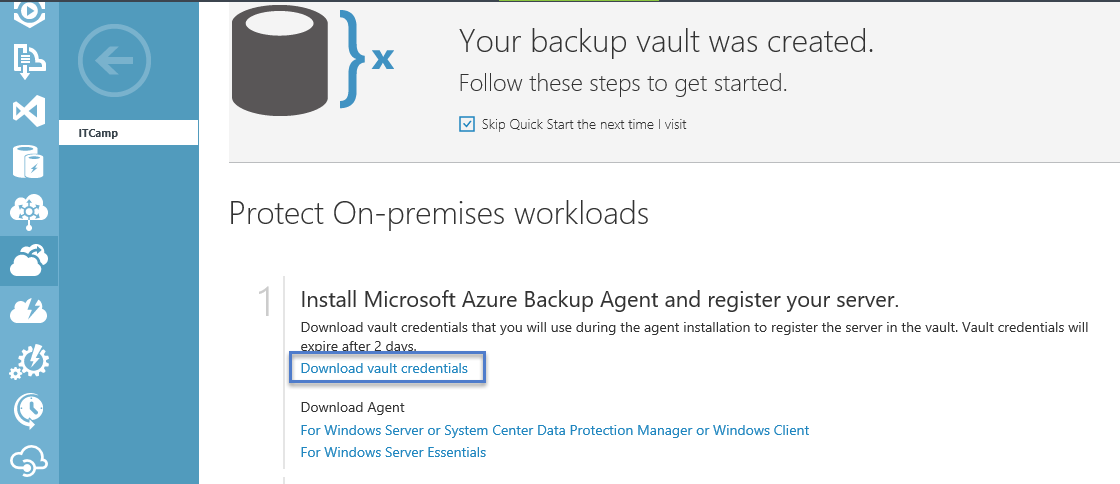
## Download the vault credential file

The vault credential file is downloaded through a secure channel from the Azure portal. The Azure Backup service is unaware of the private key of the certificate and the private key is not persisted in the portal or the service. Use the following steps to download the vault credential to a local machine.

1. If necessary, sign in to the [Management Portal](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq) and click **Recovery Services** in the left navigation pane and select the backup vault which you have created.
2. Click the cloud icon to get to the Quick Start view of the backup vault.



1. On the Quick Start page, click **Download vault credentials**. The portal generates the vault credential file which is made available for download.



1. The portal will generate a vault credential using a combination of the vault name and the current date. Click **Save** to download the vault credentials to the local account's downloads folder, or select Save As from the Save menu to specify a location for the vault credentials.

#### Notes

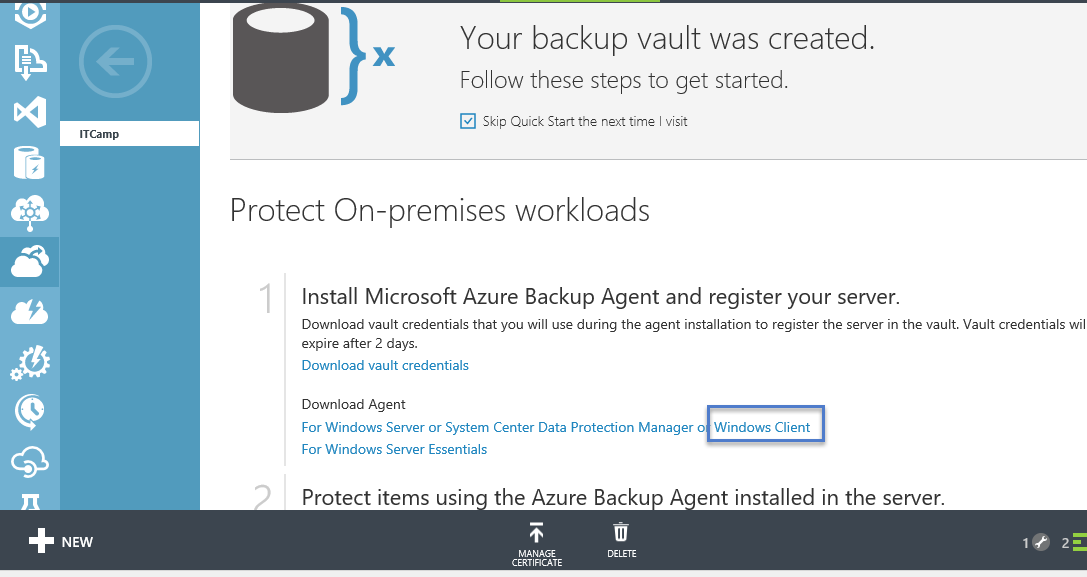
* As of March 2015, users do not have a programmatic (eg: PowerShell) way of downloading vault credentials.
* Ensure that the vault credentials are saved in a location which can be accessed from your machine. If it is stored in a file share/SMB, check for the access permissions.
* The vault credentials file is used only during the registration workflow.
* The vault credentials file expires after 48hrs and can be downloaded from the portal.
* Refer to the Azure Backup [FAQ](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq) for any questions on the workflow.

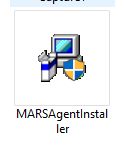
## Registering your Windows Client machine

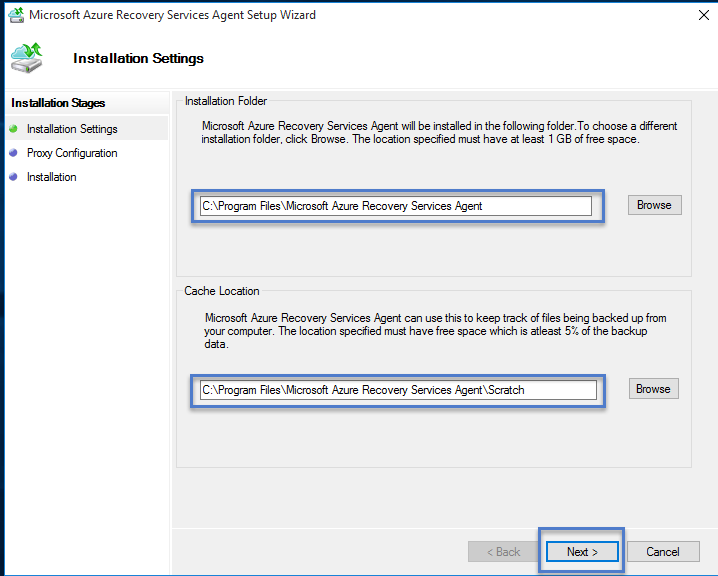
#### Download, install and register the Azure Backup agent

After creating the Azure Backup vault, an agent should be installed on each of your on-premises servers (Windows Server, Windows client or System Center Data Protection Manager server) which enables you to backup data and applications to Azure. This article covers the steps required to setup the Azure Backup agent on a Windows Server or Windows client machine.

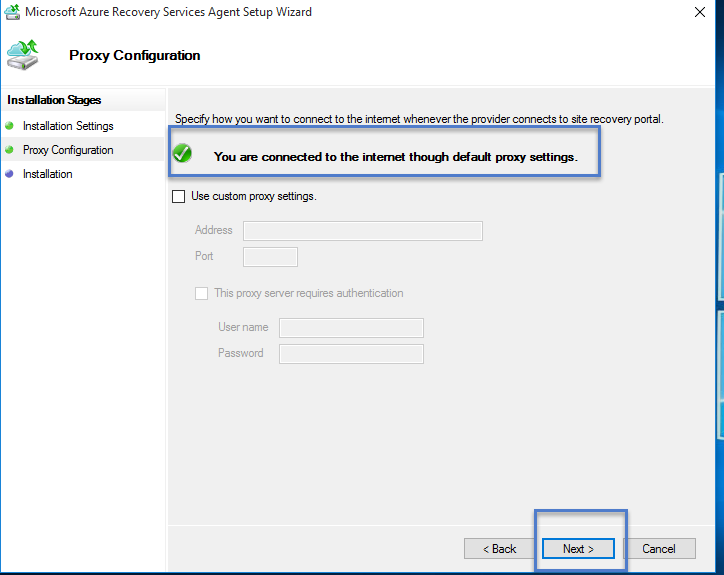
1. If necessary, sign in to the [Management Portal](https://manage.windowsazure.com/), click **Recovery Services**, then select the backup vault that you want to register with a server. The Quick Start page for that backup vault appears.



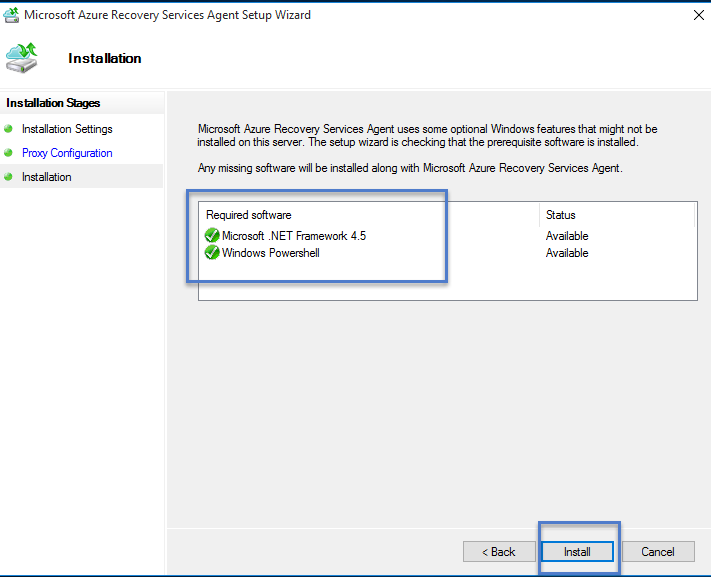
1. On the Quick Start page (below the “Download vault credentials”), click **For Windows Server or System Center Data Protection Manager or Windows client** under **Download Agent** option. Click **Save** to copy it to the local machine.
2. Once the agent is downloaded, double click **MARSAgentInstaller.exe** to launch the installation of the Azure Backup agent.
3. Choose the installation folder and folder required for the agent. The cache location specified must have free space which is at least 5% of the backup data.



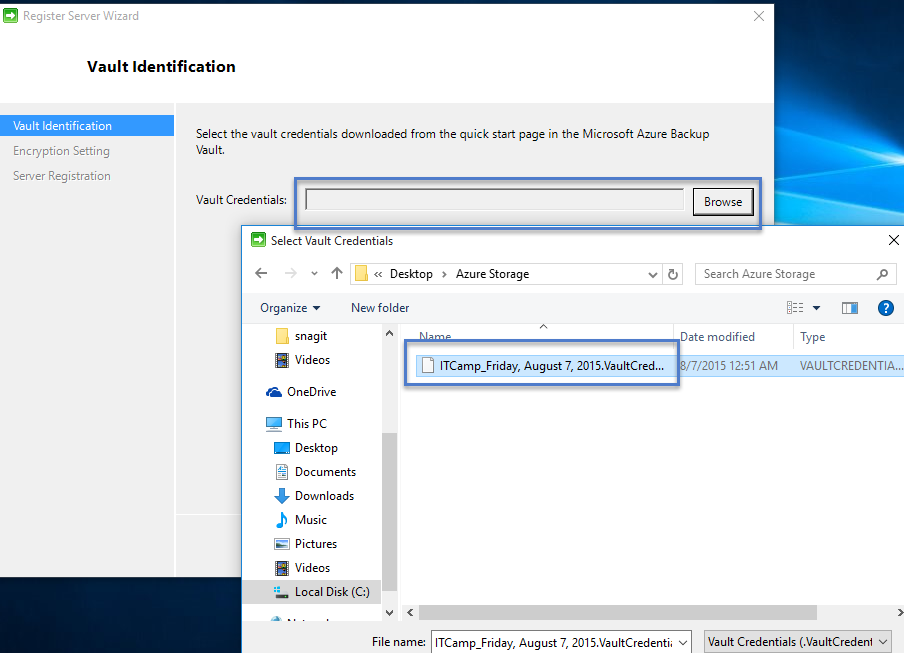
1. If you use a proxy server to connect to the internet, in the **Proxy configuration** screen, enter the proxy server details. If you use an authenticated proxy, enter the user name and password details in this screen.



1. The Azure Backup agent install .NET Framework 4.5 and Windows PowerShell (if it’s not available already) to complete the installation.

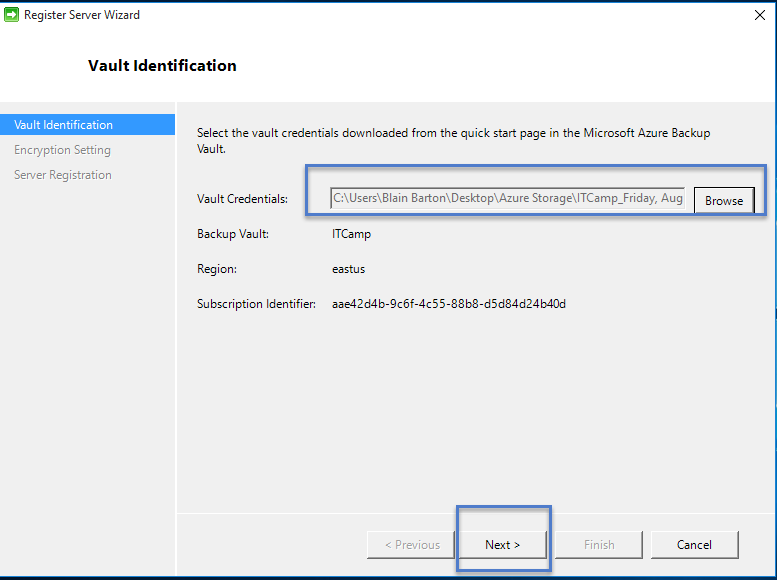


1. Once the agent is installed, click the **Proceed to Registration** button to continue with the workflow.
2. In the vault credentials screen, browse to and select the vault credentials file which was previously downloaded.



**NOTE:**

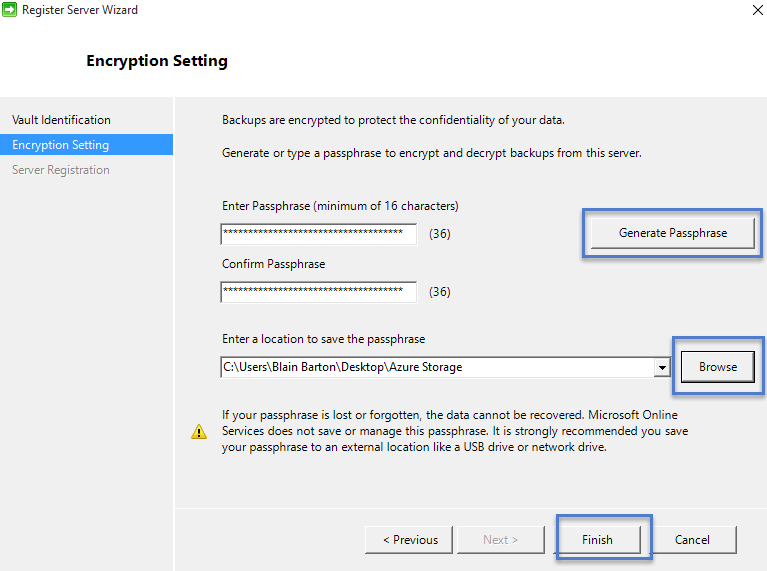
The vault credentials file is valid only for 48 hrs (after it’s downloaded from the portal). If you encounter any error in this screen (e.g “Vault credentials file provided has expired”), login to the Azure portal and download the vault credentials file again.



Ensure that the vault credentials file is available in a location which can be accessed by the setup application. If you encounter access related errors, copy the vault credentials file to a temporary location in this machine and retry the operation.

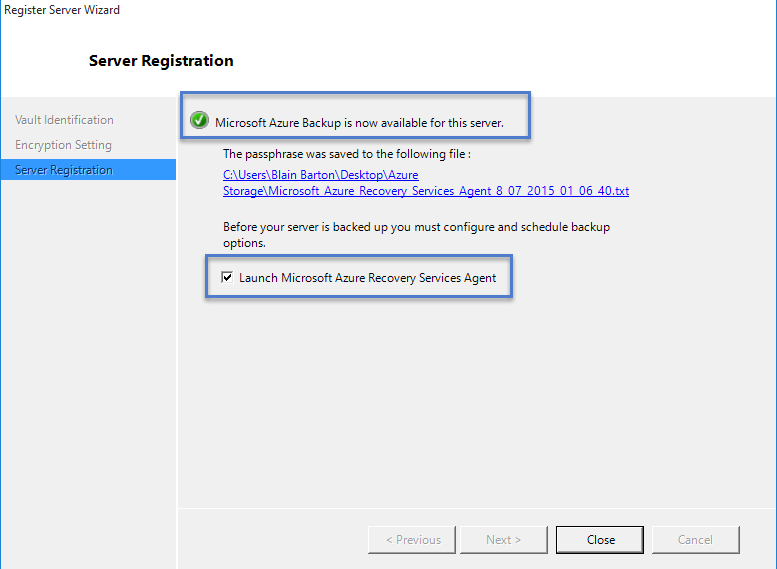
If you encounter an invalid vault credential error (e.g “Invalid vault credentials provided". The file is either corrupted or does not have the latest credentials associated with the recovery service”, retry the operation after downloading a new vault credential file from the portal. This error is typically seen if the user clicks on the Download vault credential option in the Azure portal, in quick succession. In this case, only the second vault credential file is valid.

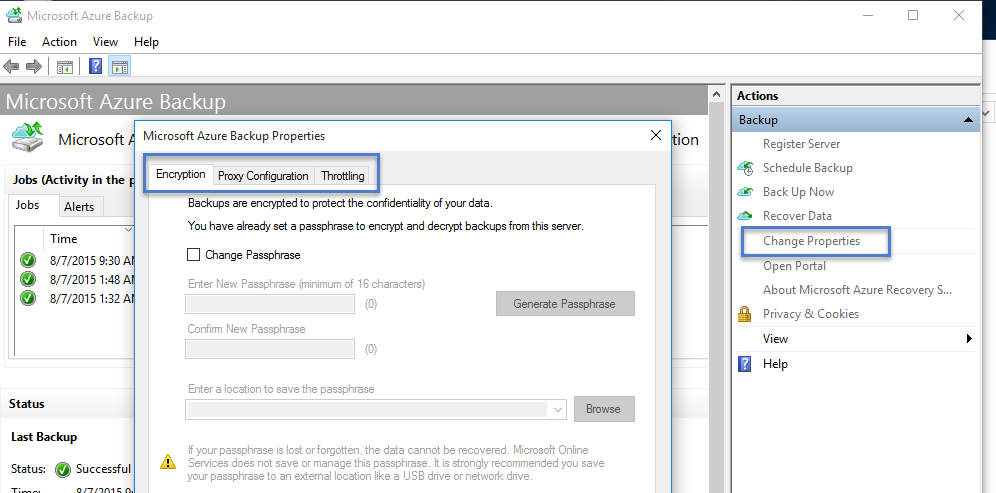
1. In the **Encryption setting** screen, you can either generate a passphrase or provide a passphrase (minimum of 16 characters) and remember to save the passphrase in a secure location.



WARNING:

If the passphrase is lost or forgotten; Microsoft cannot help in recovering the backup data. The end user owns the encryption passphrase and Microsoft does not have any visibility into the passphrase which is used by the end user. Please save the file in a secure location as it would be required during a recovery operation.

1. Once you click the **Finish** button, the machine is registered successfully to the vault and you are now ready to start backing up to Microsoft Azure.
2. You can modify the settings specified during the registration workflow by clicking the **Change Properties** option in the Azure Backup mmc snap in.

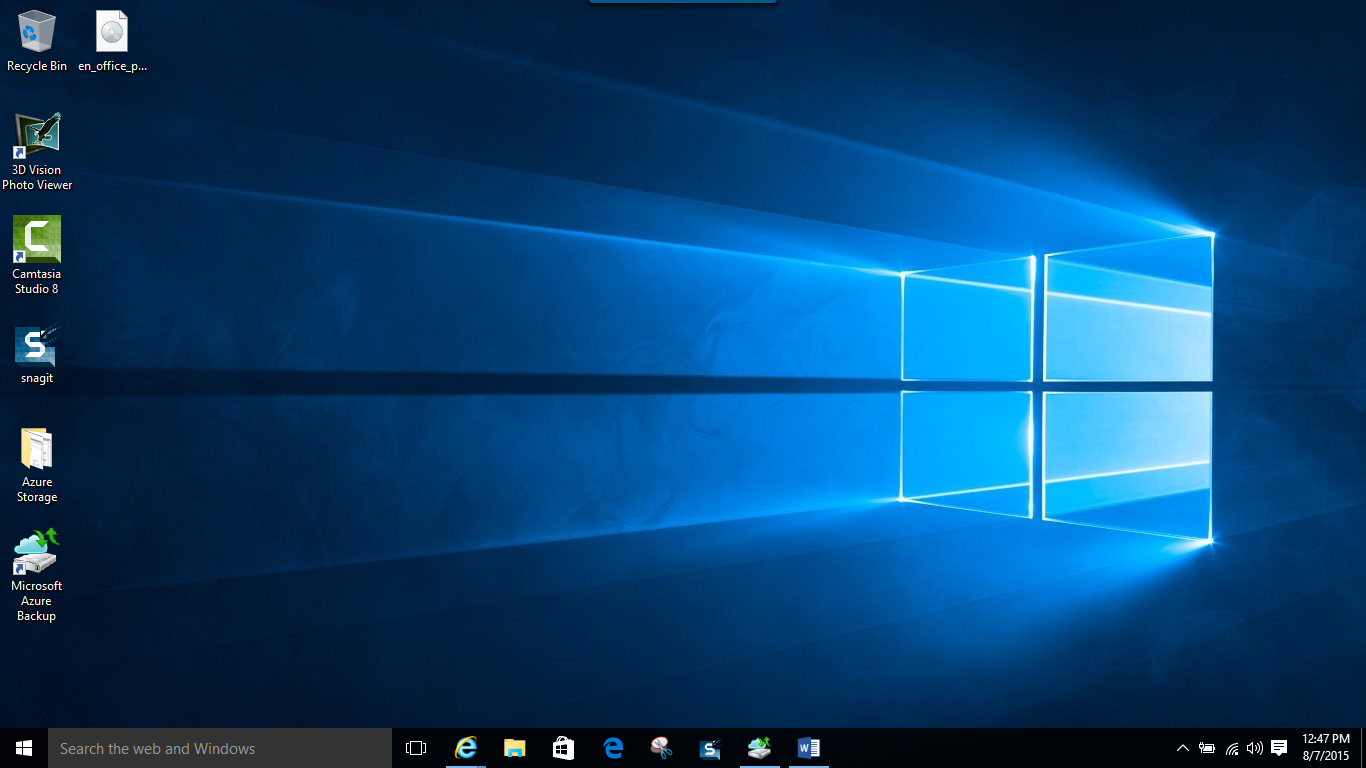


## Backup and restore from a Windows server or Windows client machine

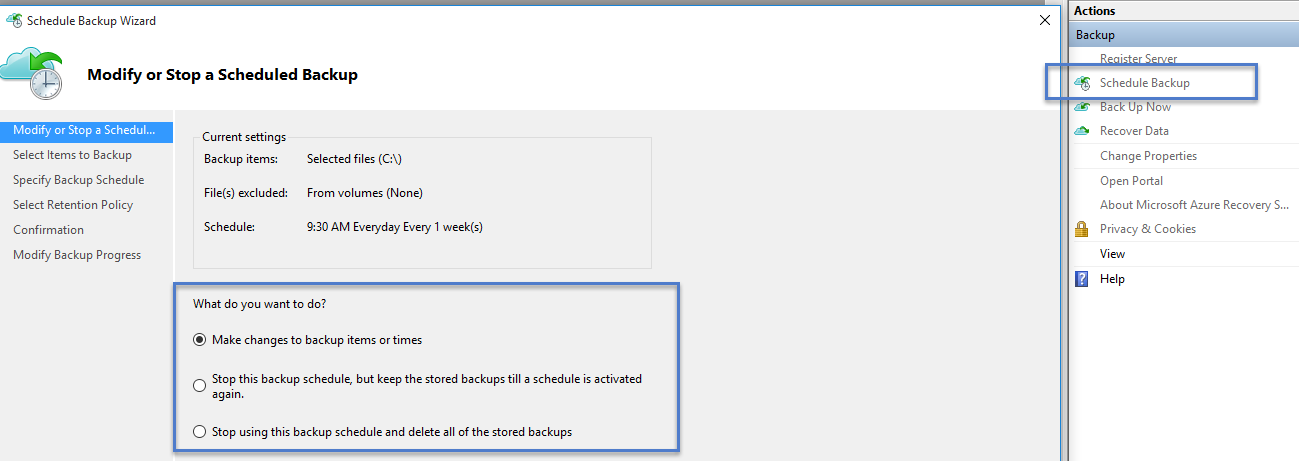
This lab covers the steps required to back up from a Windows server or a Windows client machine. It also covers the steps required to restore the backed up files on the same machine and the steps required to restore the backed up files on any other machine.

#### Scheduling and Backing Up files

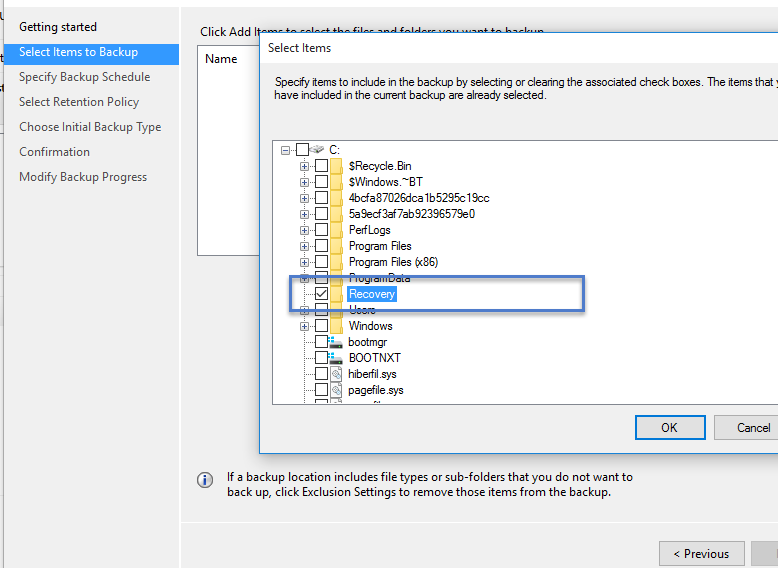
1. Once the machine is registered, open the **Microsoft Azure Backup** from the Desktop.

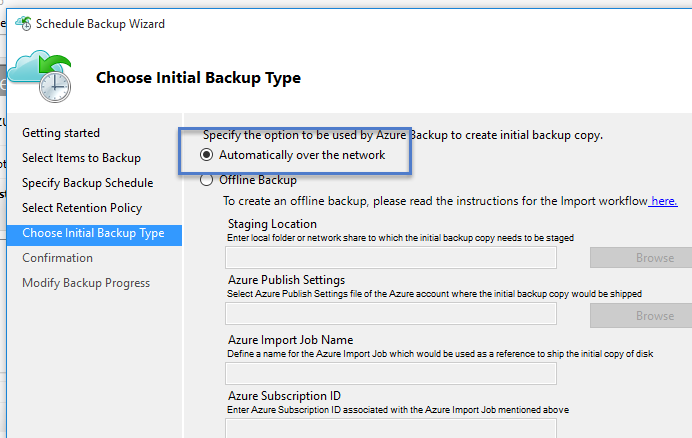


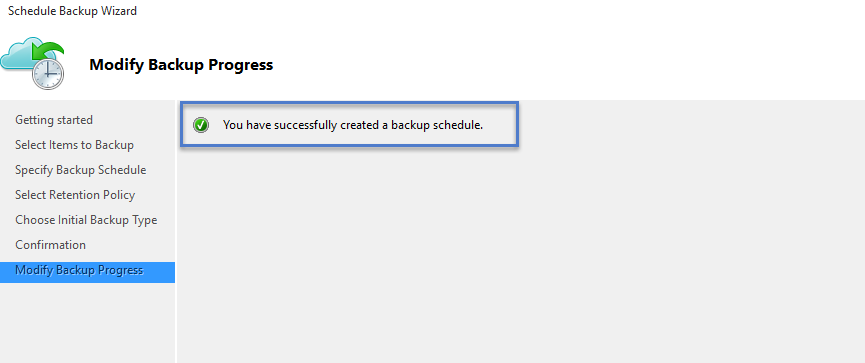
1. Click on **Schedule Backup** (This is for modifying a job and you might not see this for the first time.**)**



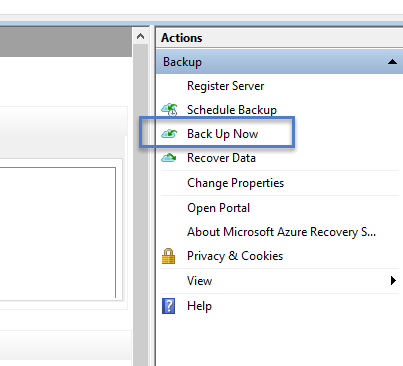
1. Select the items which you wish to back up. Azure Backup on a Windows Server/Windows Client (i.e without System Center Data Protection Manager) enables you to protect files and folders. **Create and pick a folder you want to backup.** In this case we took the c:\recovery folder.

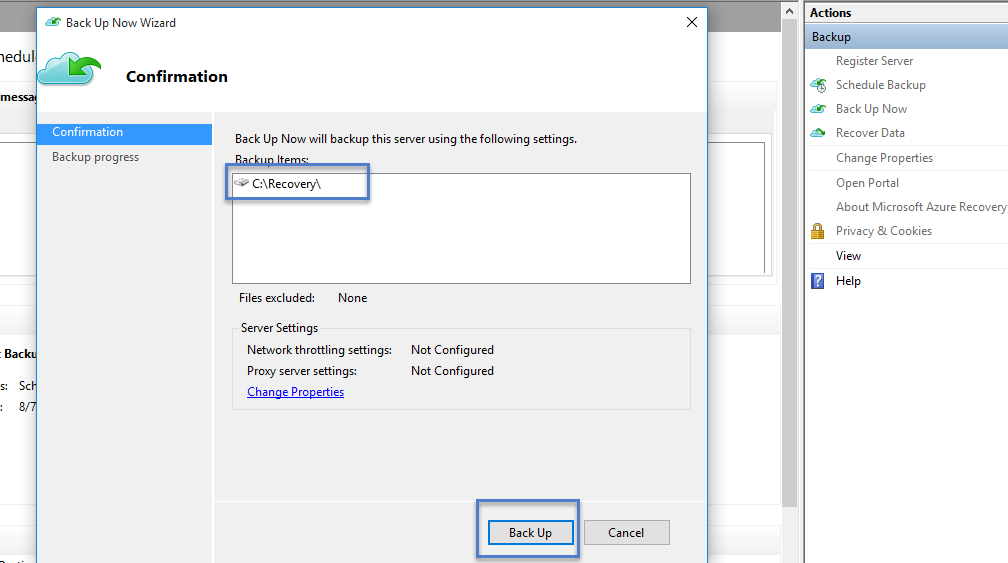


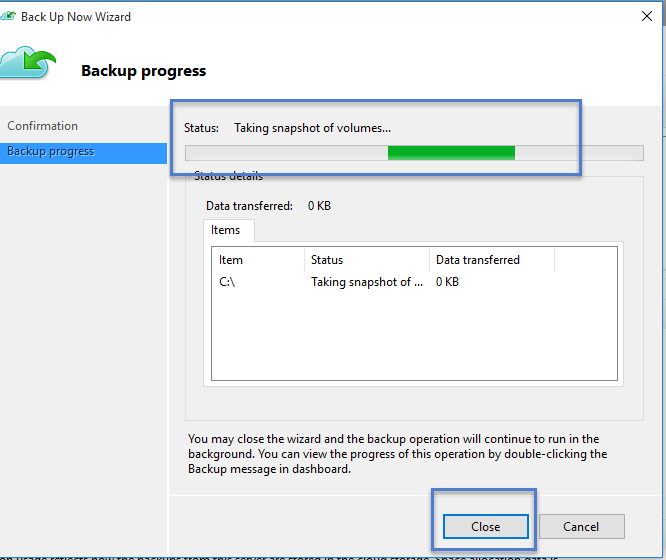
1. Specify the backup schedule and retention policy
2. Choose the method of sending the initial backup. Your choice of completing the initial seeding is dependent on the amount of data you wish to back up and your internet upload link speed. If you plan to back up GB’s/TB’s of data over a high latency, low bandwidth connection, it is recommended that you complete the initial backup by shipping a disk to the nearest Azure data center. If you have a sufficient bandwidth connection we recommend that you complete the initial backup over the network.

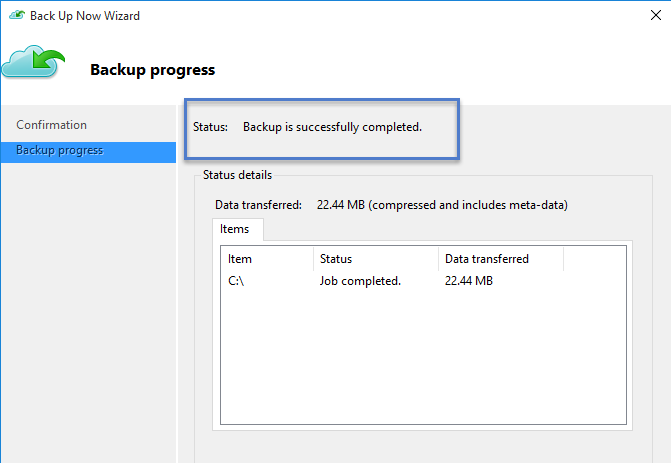


1. Once the process completes, go back to the mmc snap in and click **Back up Now** to complete the initial seeding over the network.







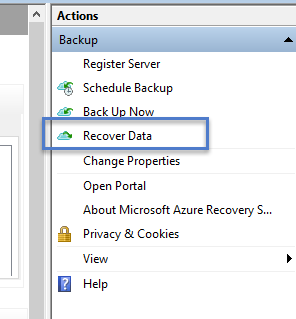


1. Once the initial seeding is completed, the **Jobs** view in the Azure Backup console indicates the status.

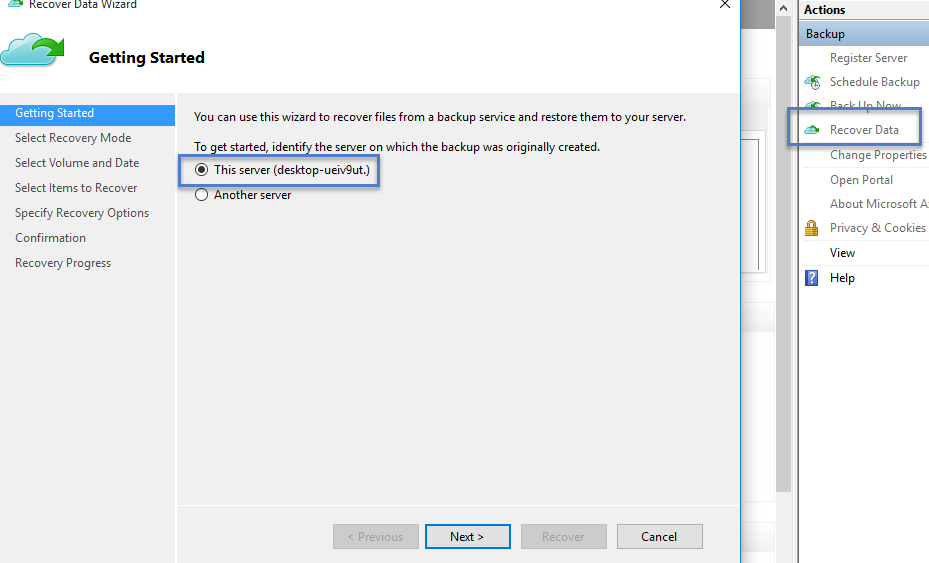
#### Recover data on the same machine

If you accidentally deleted a file and wish to restore the file/volume on the same machine (from which the backup is taken), the following steps will help you recover the data.

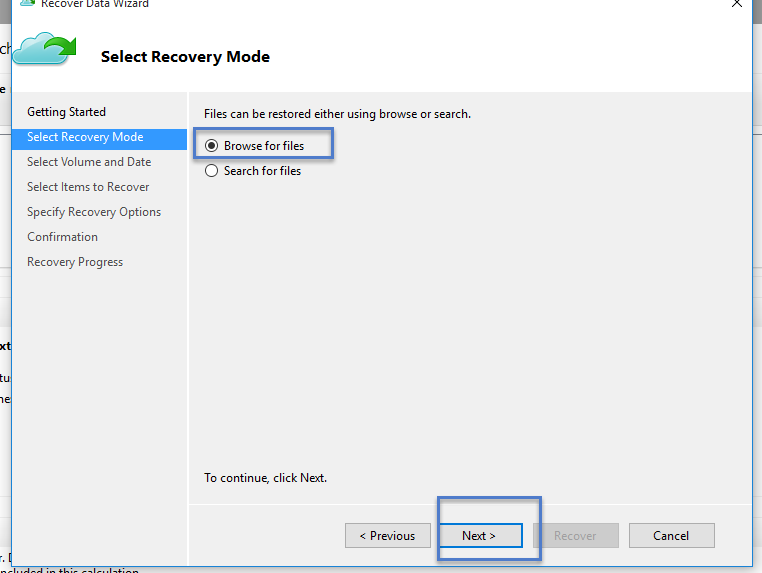
1. Click **Recover Data** to initiate the workflow.



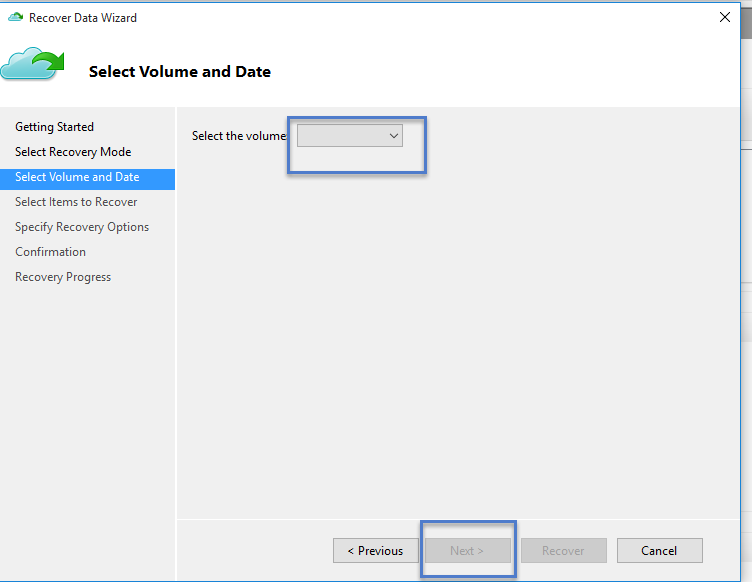
1. Select **This server (*yourmachinename*)** option as you plan to restore the backed up file on the same machine.



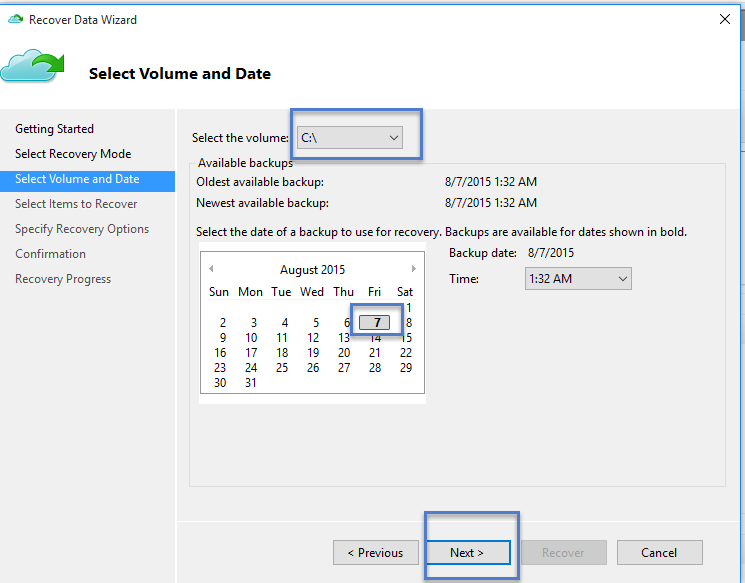
1. You can choose to **Browse for files** or **Search for files**. Leave the default option if you plan to restore one or more files whose path is known. If you are not sure about the folder structure but would like to search for a file, pick the **Search for files** option. For the purpose of this section, we will proceed with the default option.



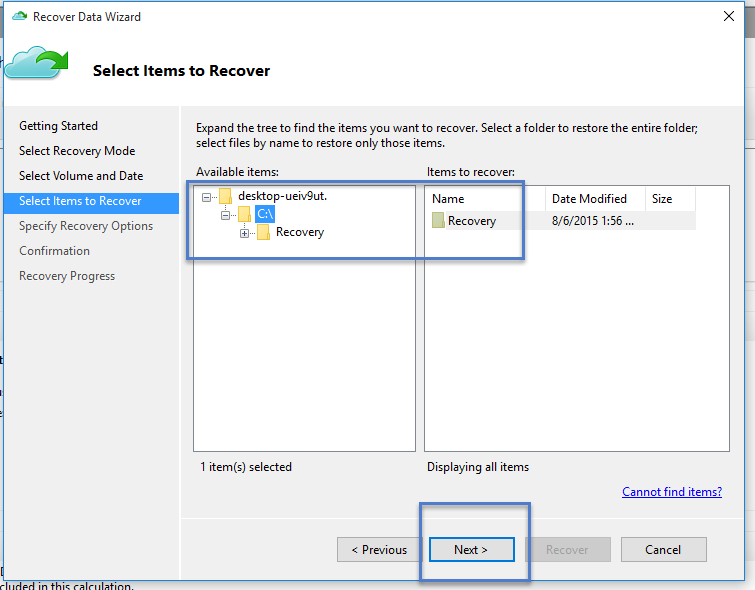
1. Select the volume from which you wish to restore the file.



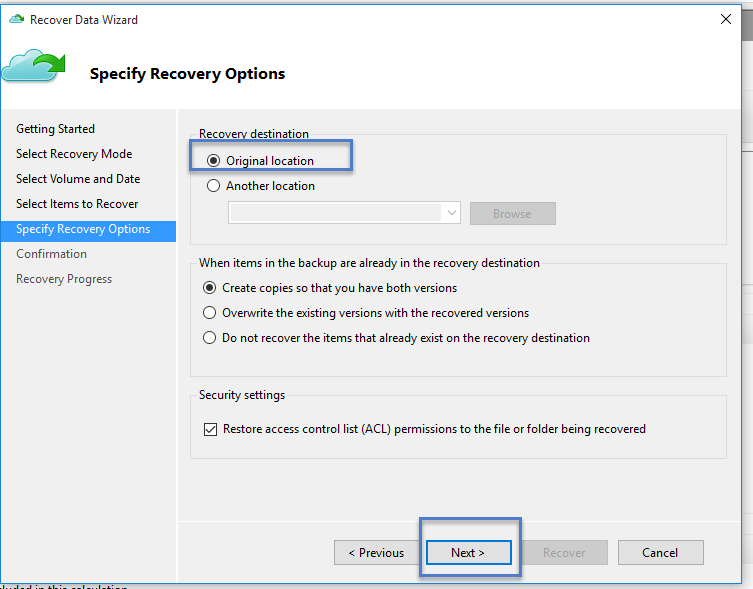
1. The screen enables you restore from any point in time. Dates which appear in **bold** in the calendar control indicate the availability of a restore point. Once a date is selected, based on your backup schedule (and the success of a backup operation), you can select a point in time from the **Time** drop down.



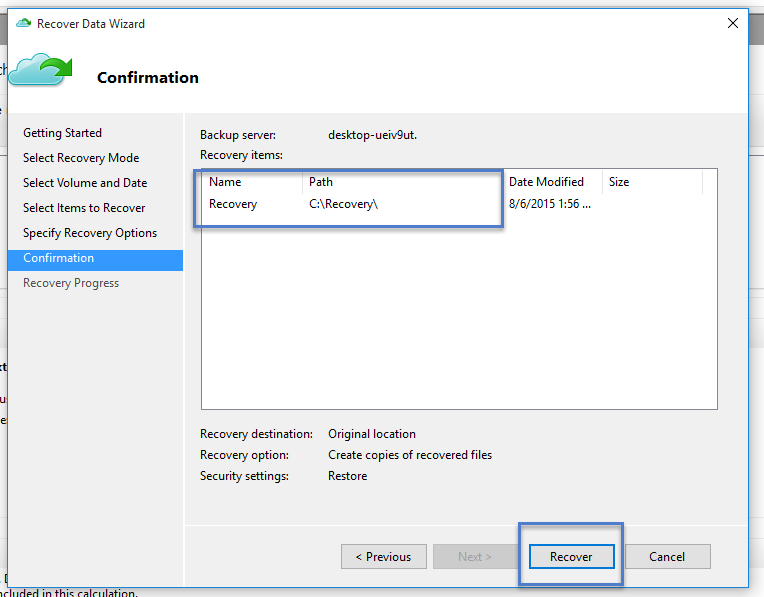
1. Select the items you wish to recover. You can multi-select folders/files which you wish to restore.



1. Specify the recovery parameters.

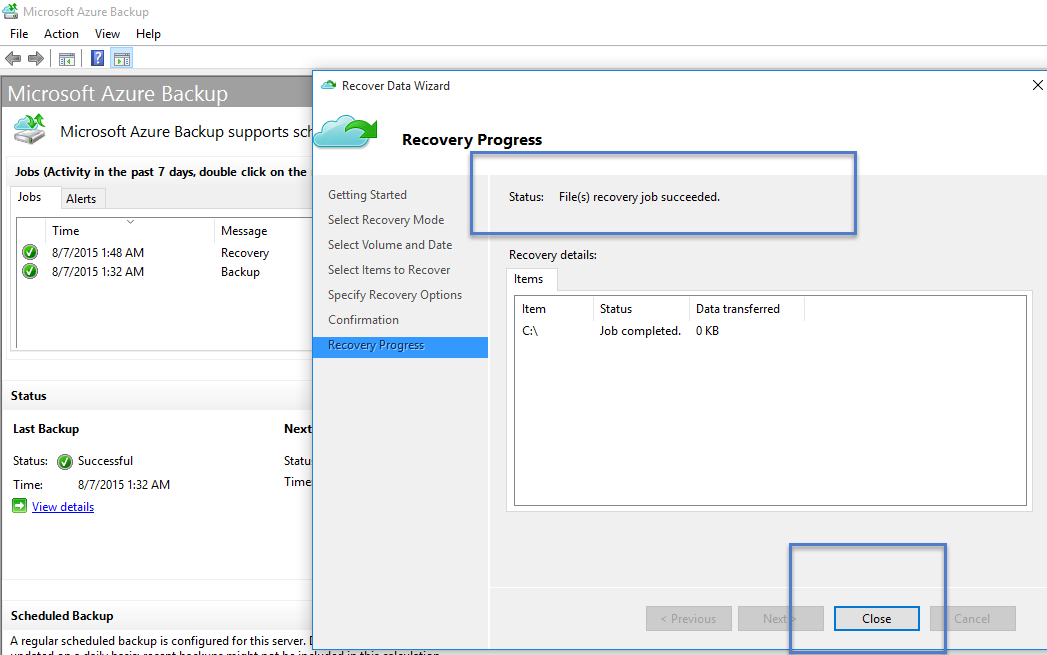


* + You have an option of restoring to the original location (in which the file/folder would be overwritten) or to another location in the same machine.
  + If the file/folder which you wish to restore, exists in the target location, you have the option to either create copies (two versions of the same file), or overwrite the files in the target location or skip the recovery of the files which exist in the target.

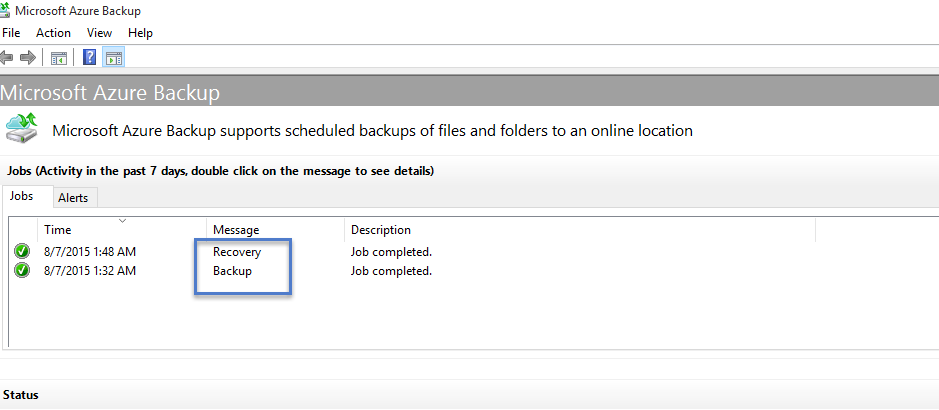


* + It is highly recommended that you leave the default option of restoring the ACLs on the files which are being recovered.

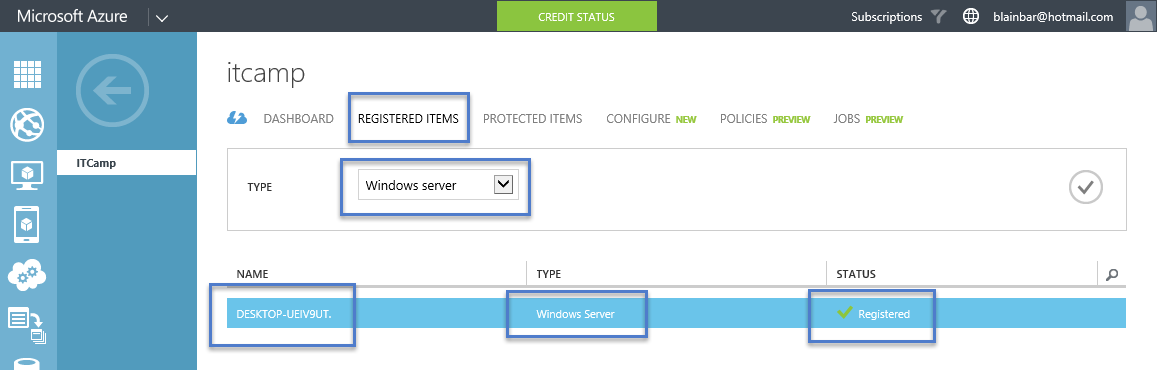
1. Once these inputs are provided, the recovery workflow starts which restores the files to this machine.



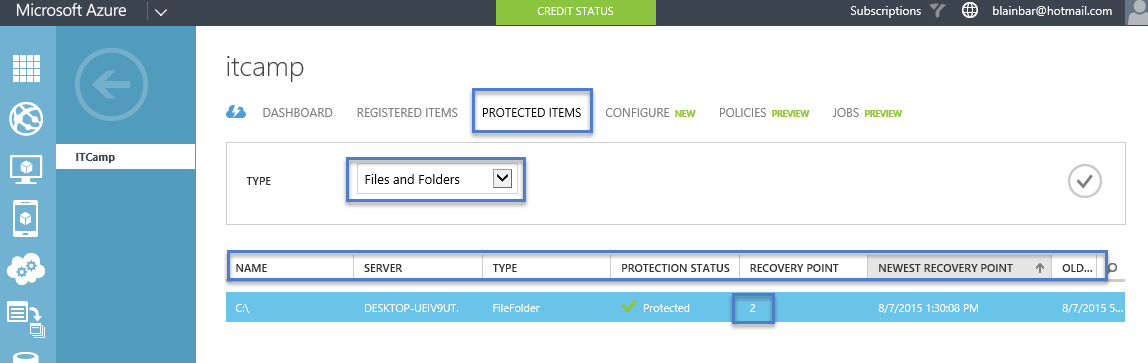
Here you can see the Backup and Recovery status.



If you go back into the Microsoft Azure Recovery Services Backup Vault you can see the **Registered Items**, even though it is a backup up of the client, it will say “Windows Server”.



You can also see the **Protected Items** but not the individual files themselves as the folders and files are stored in blog storage. You can only see the individual folders and files from the Azure Backup Agent on the physical machine.



This concludes “Backing up your files and folders with Microsoft Azure Recovery Services Backup Vault” for Windows Clients, Windows Servers and System Center Data Protection Manager. For more information on Microsoft Azure Recovery Services Backup Vault go to: <http://azure.microsoft.com/en-us/services/backup> For FAQ’s on Microsoft Azure Backup go to: [https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq/)

# Lab 11 Creating and Managing Website & Services

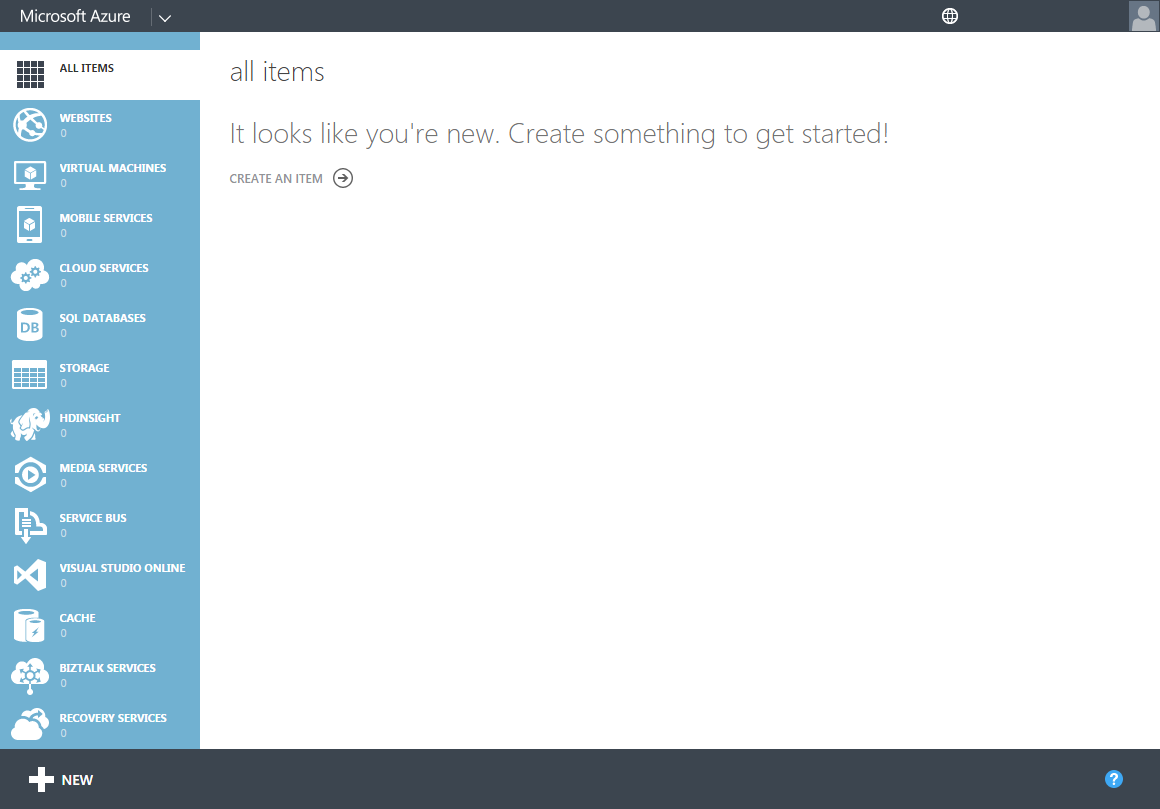
The Azure Management Portal is your one-stop-shop for creating and managing new cloud resources, like websites, virtual machines, and storage accounts. Once you get started, the portal will be your home to configure, monitor, and scale your resources with ease and agility.

#### Create Website

In this task you will walk through the different pieces of the Azure Management Portal.

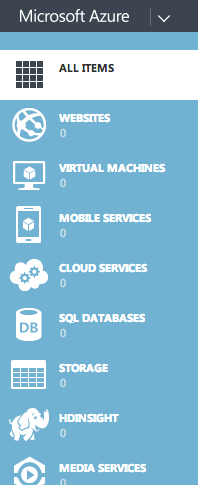
1. Open you browser and navigate to [http://manage.windowsazure.com](http://manage.windowsazure.com/).
2. Enter your credentials to access your Azure Subscription.

You will land on the portal's home view. By default this view will show all the items you have ever created under your subcription.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/portal-landing-page.png?raw=true)

Management Portal - Landing Page

1. On the left side, notice the sidebar displaying all the available services and tools. Clicking any of these items will filter the list by that specific type.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/portal-left-sidebar.png?raw=true)

Left Sidebar

1. Look at the portal's footer and notice the **NEW** button on the left and the **Help** button on the right. You will see more about these two items as you move on to the other tasks.

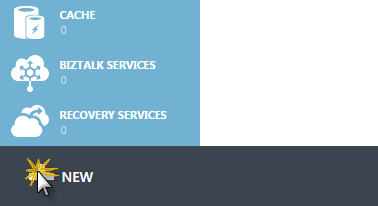
[New Button](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/portal-new-button.png?raw=true)

NEW and Help Buttons

## Creating new elements and services

In this task you will go through the process of creating a new element for your subscription. In particular, you will create a new website using the **Create Wizard**.

1. Click the **NEW** button located at the bottom left part of the screen.



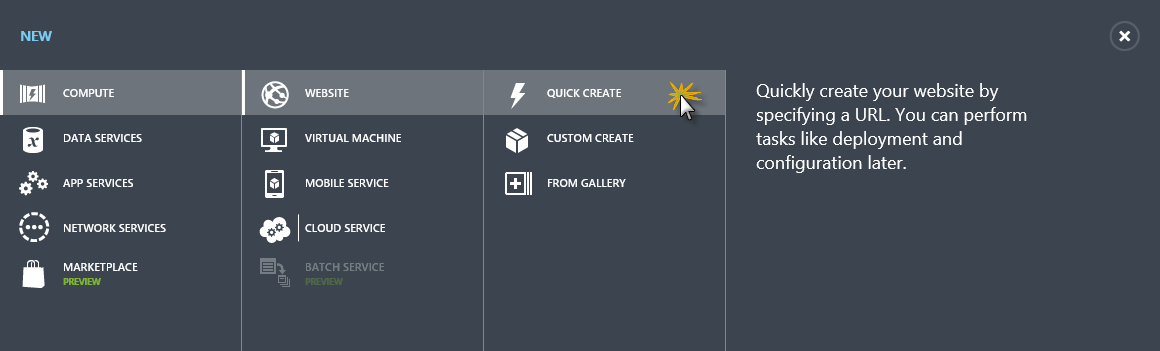
NEW Button Clicked

This will display the Create Wizard. In this section you can select the type of element, service or resource we want to create. In this case you will create a Website.

1. Click **COMPUTE**. The compute services will be displayed alongside.
2. Click **WEBSITE**.

Three options will be shown.

* + **QUICK CREATE**: This option will allow you to setup your website with the minimum amount of steps.
  + **CUSTOM CREATE**: You will have the chance to create a SQL Database to attach to this website and setup a continuous deployment source.
  + **FROM GALLERY**: The gallery features a list of templates ready to jumpstart your website.

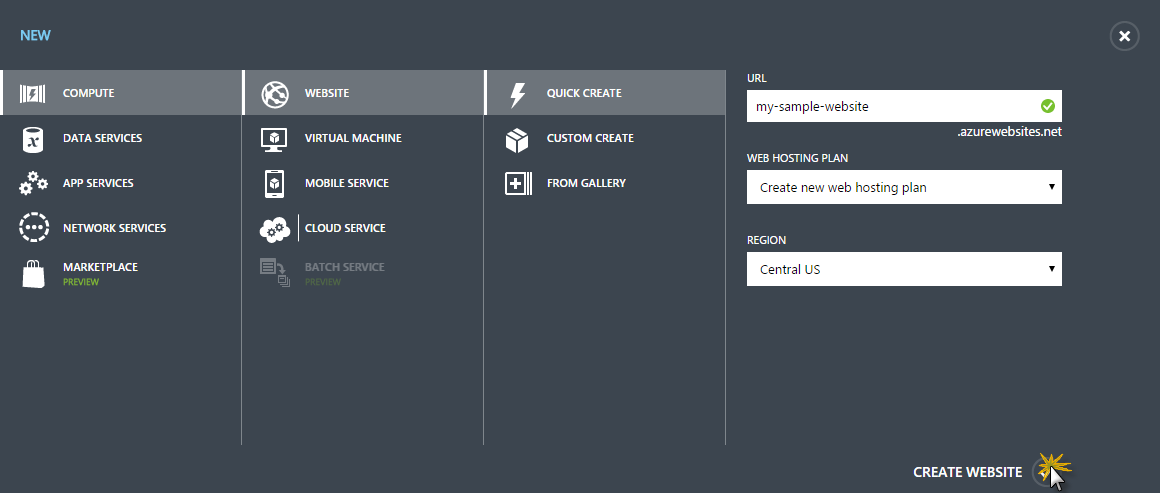
Website Creation Options

1. Click **QUICK CREATE**.

The creation form is presented. Here you will select the URL for your website and the region where you would like to deploy. It is recommended to select the region which is closest to your audience; for this task leave the field as is.

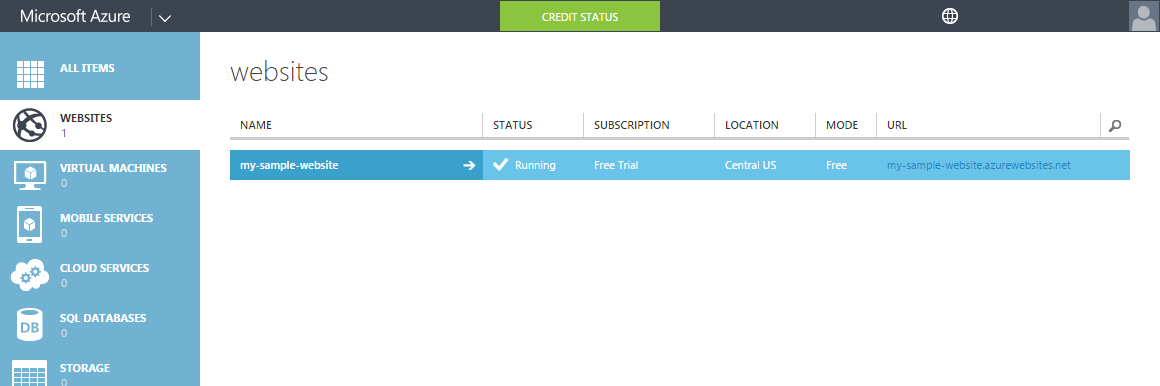
1. Enter the **URL** for your website, and click **CREATE WEBSITE**.

**Note:** The website URL has to be unique since it will be of public access.



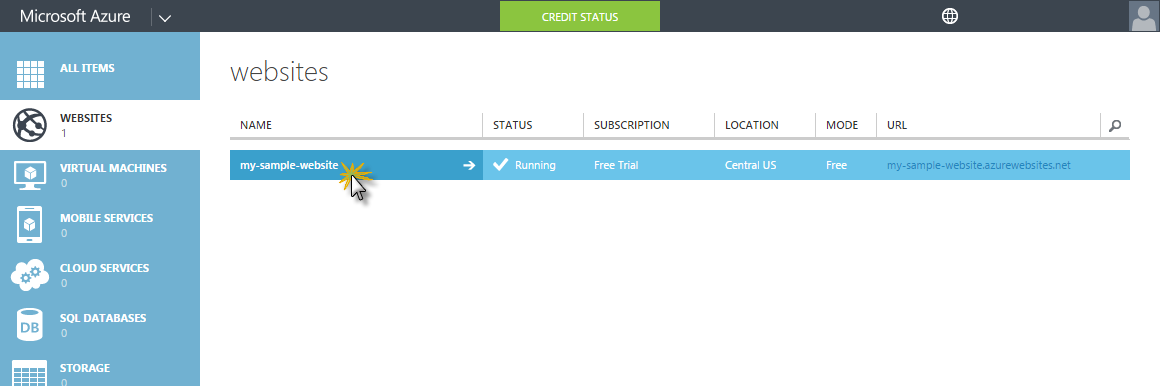
Creating the Website

1. After a few minutes the website will be created and you will see a notification on the status bar. The **WEBSITES** item is selected on the sidebar, and the asset just created is displayed.



Website Created

1. Click the site name you have just created to navigate to the website's Quick Start Management page.

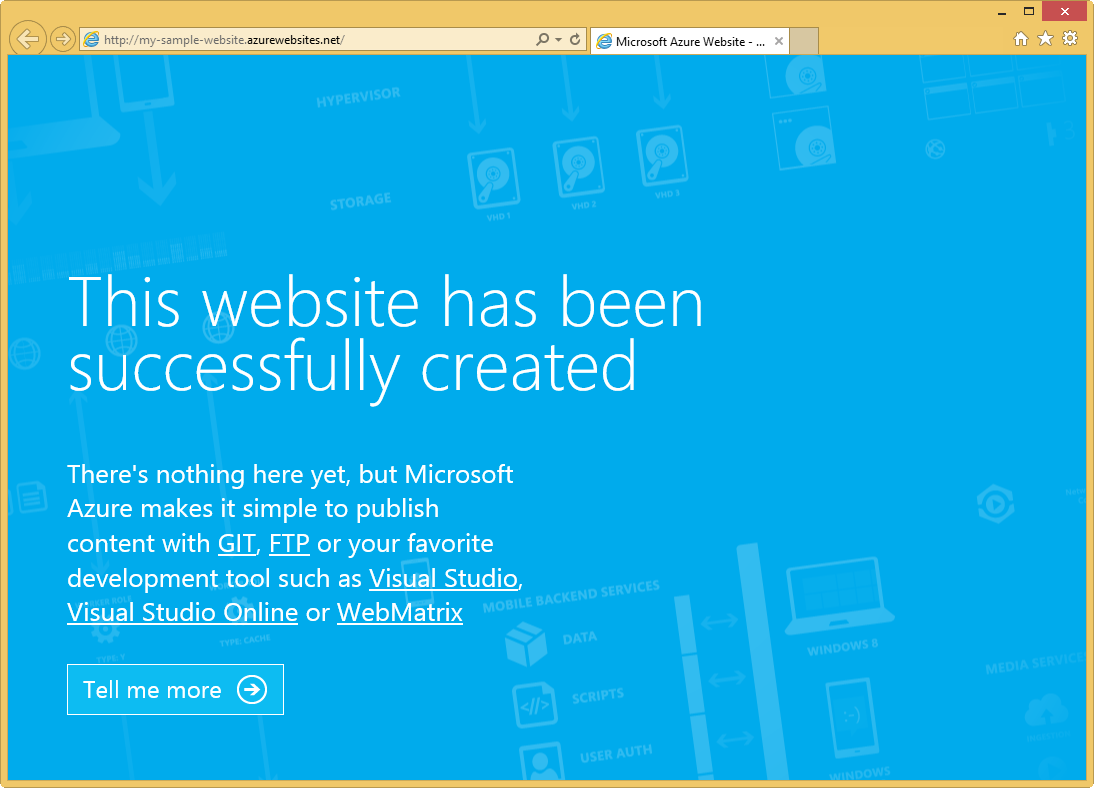


Entering the site's management page

1. Click **BROWSE**, located at the bottom of the page, to navigate to the site.

Clicking Browse to view the site

Clicking Browse



Browsing the Website

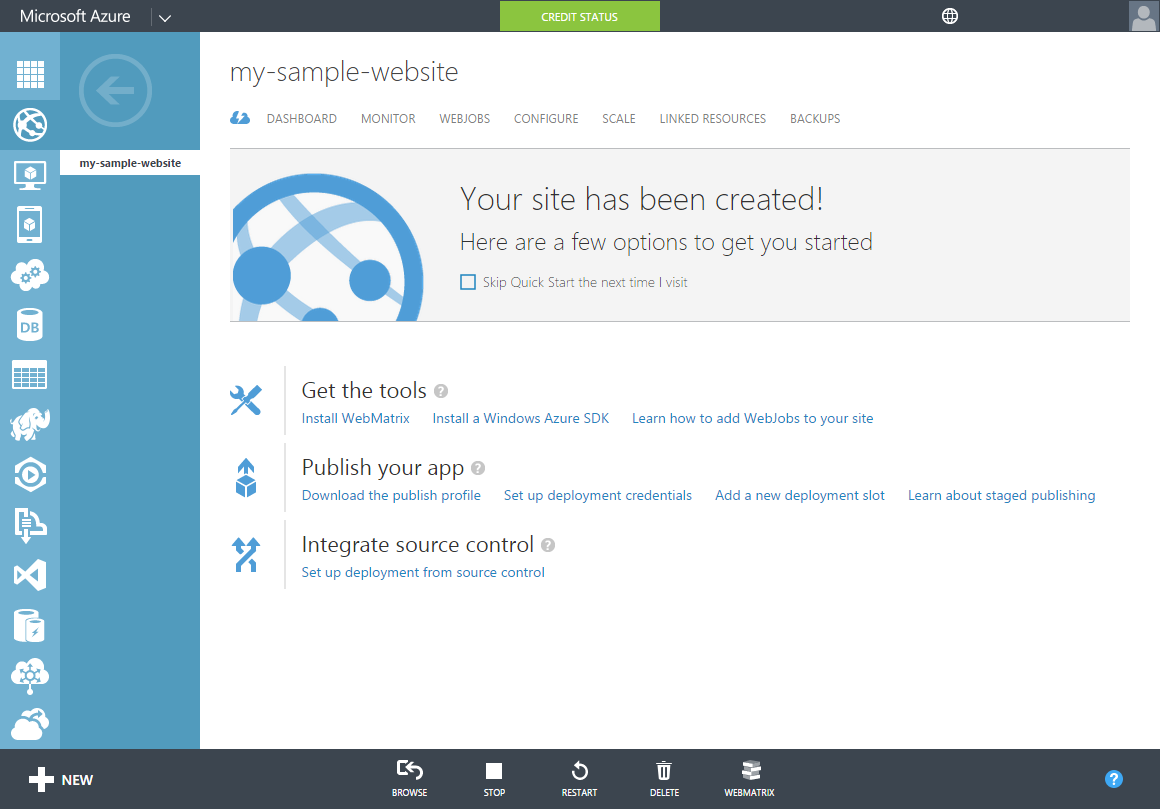
1. Close the website and return to the **Management Portal**.

## Managing allocated resources

In this task you will go through the available options for managing the recently created website.

1. If not already in the Quick Start Management page, click the website's name to display it.

This page provides quick access to important actions related to managing the deployment of a site in Windows Azure. This is also the default landing page in the portal for a newly created website.



Website's Quickstart Management page

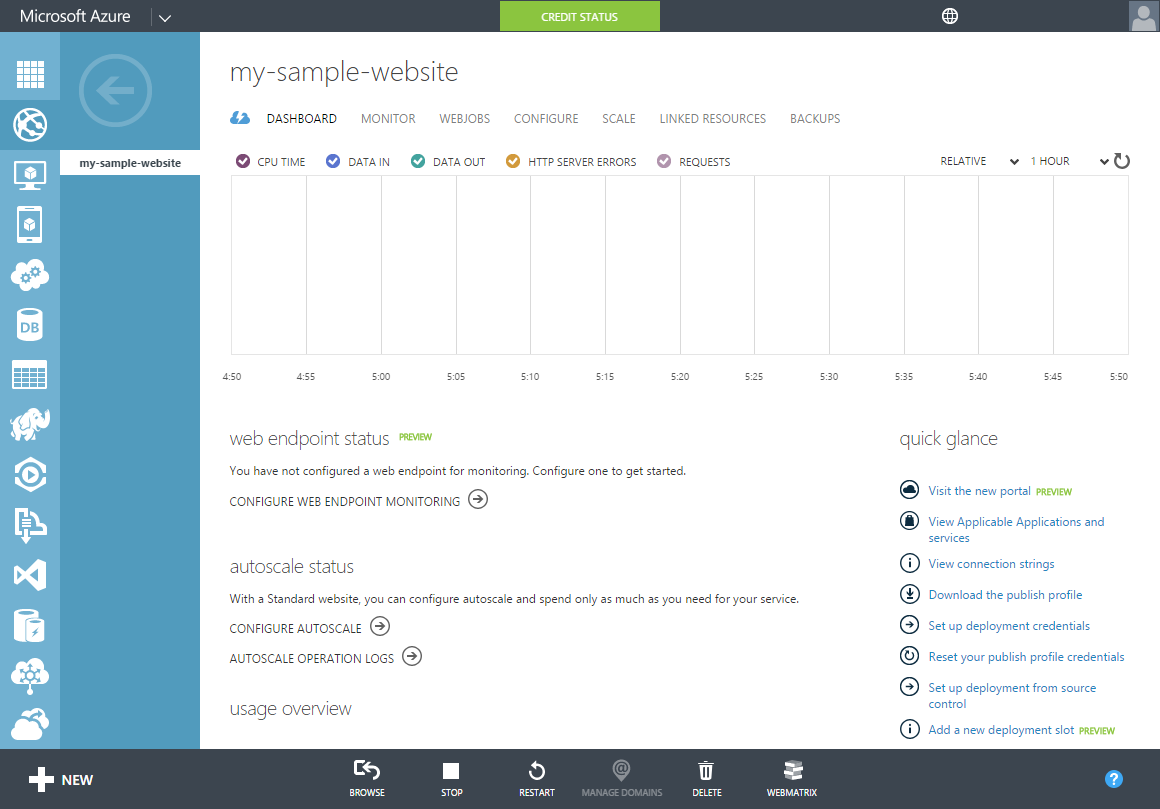
1. Notice the commands located at the bottom of the page. These are:
   * **BROWSE**: To navigate to the current deployed version of the website
   * **STOP**: To stop the website's deployment
   * **RESTART**: To restart the website's deployment
   * **DELETE**: To delete the website
   * **WEBMATRIX**: Allows to install WebMatrix, Microsoft's new one-stop website authoring tool that lets you create, edit, and publish websites easily.
2. Look at the top bar to see the different sections available. These sections are:
   * Dashboard
   * Monitor
   * Webjobs
   * Configure
   * Scale
   * Linked Resources
   * Backups

The rest of the task will describe the more important ones.

**Note**: For more information about all these options, see [Manage websites through the Azure Management Portal](http://azure.microsoft.com/en-us/documentation/articles/web-sites-manage/).

1. Click **DASHBOARD**.

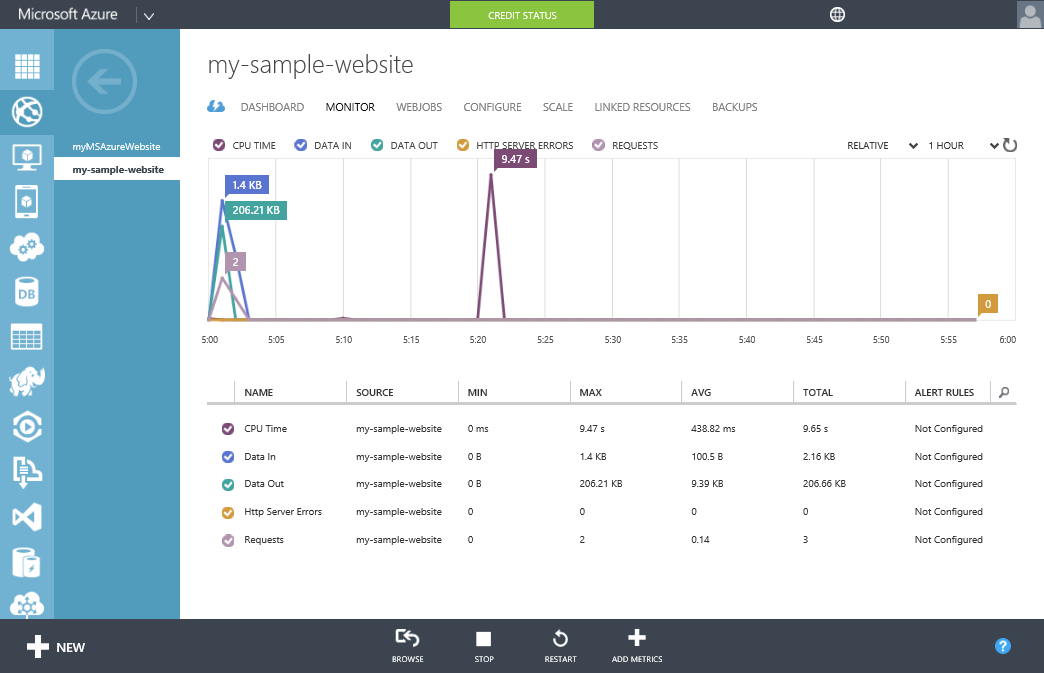
The website's dashboard will show. This view will provide you with the most important information at a glance. Ranging from a health report to usage statistics, this view provides the core details of your service.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/website-dashboard-view.png?raw=true)

The Dashboard view

1. On the top bar, click **MONITOR**.

This view allows the setup of tests to check the availability of HTTP or HTTPS endpoints, from up to three geo-distributed locations. A monitoring test fails if the HTTP response code is an error (4xx or 5xx) or the response takes more than 30 seconds. An endpoint is considered available if the monitoring tests succeed from all the specified locations.

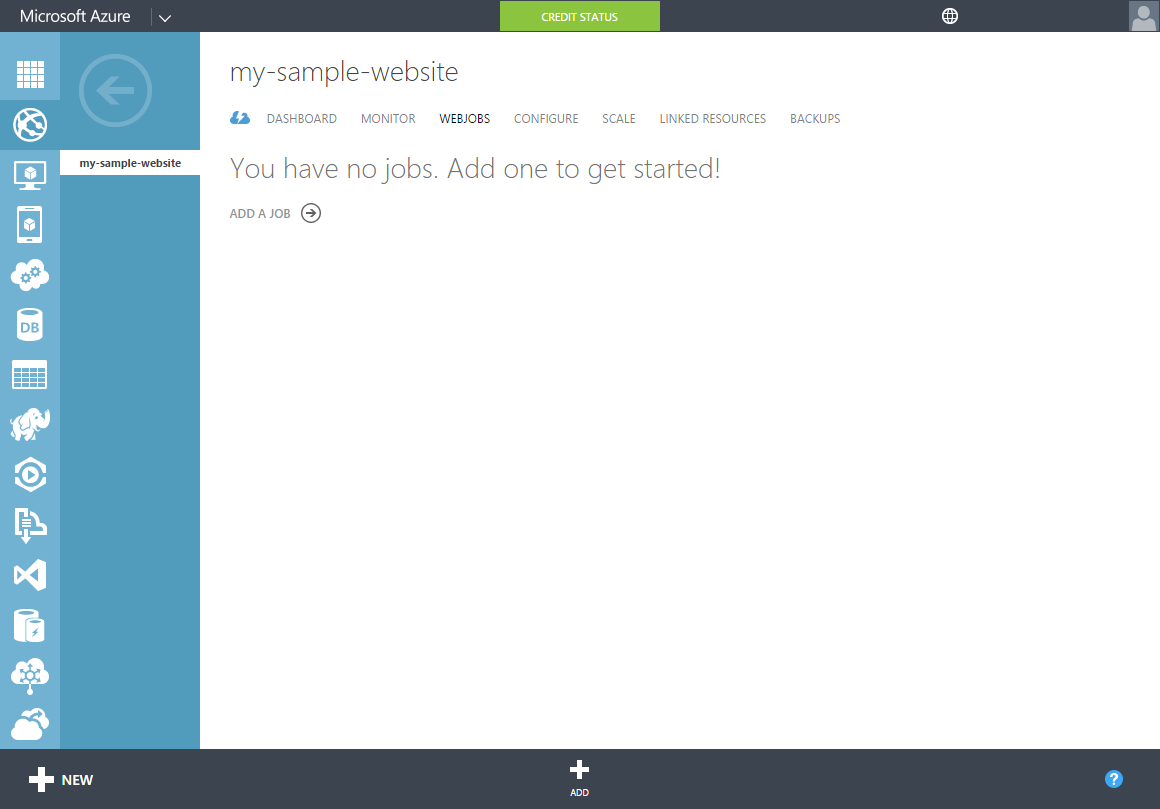
[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/website-monitor-view.png?raw=true)

The Monitor view

1. On the top bar, click **WEBJOBS**.

The WebJobs management page lets you create tasks for your website that can run on-demand, on a schedule or continuously.

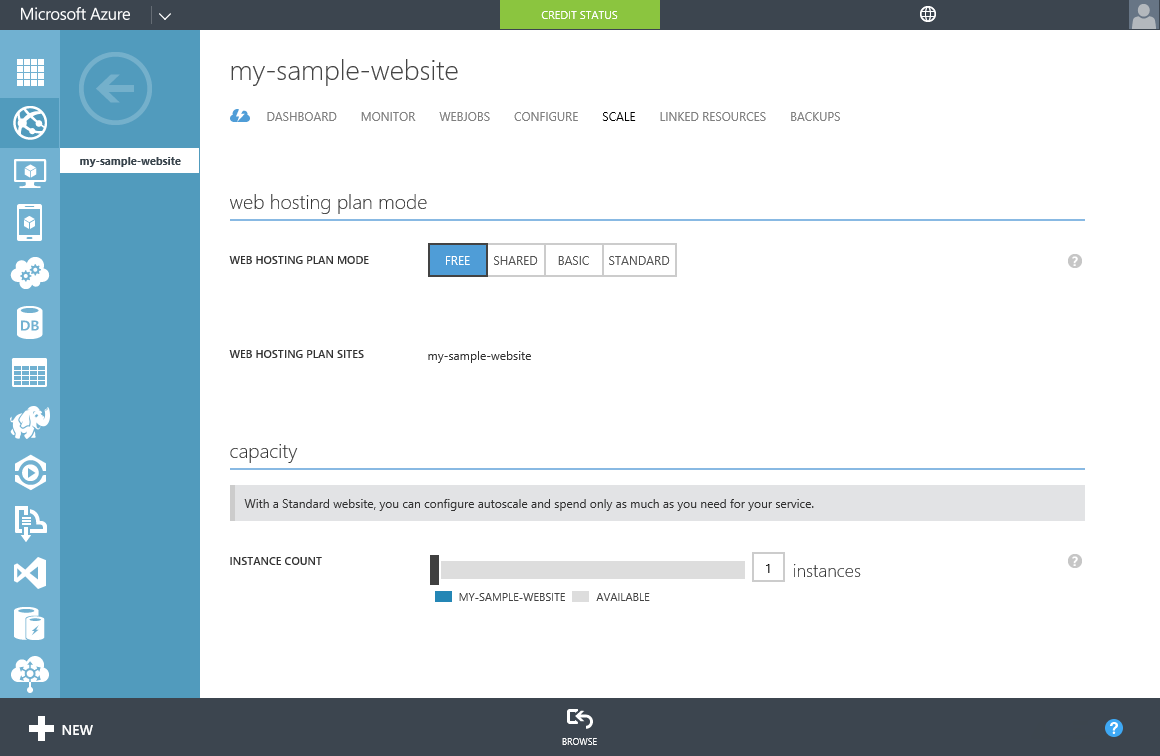
**Note**: For more information regarding the use of Webjobs, see [How to Use the WebJobs feature in Microsoft Azure Web Sites](http://azure.microsoft.com/en-us/documentation/articles/web-sites-create-web-jobs/).

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/website-webjobs-view.png?raw=true)

The Webjobs view

1. Lastly, click **SCALE** on the top bar, to go to the scaling options.

For increased performance and throughput for your websites on Microsoft Azure, you can scale your Web Hosting Plan mode from Free to Shared, Basic, or Standard. Scaling up on Azure Websites involves two related actions: changing your Web Hosting Plan mode to a higher level of service, and configuring certain settings after you have switched to the higher level of service. You can scale up or down as required. These changes take only seconds to apply and affect all websites in your Web Hosting Plan. They do not require your code to be changed or your applications to be redeployed.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/website-scale-view.png?raw=true)

The Scale view

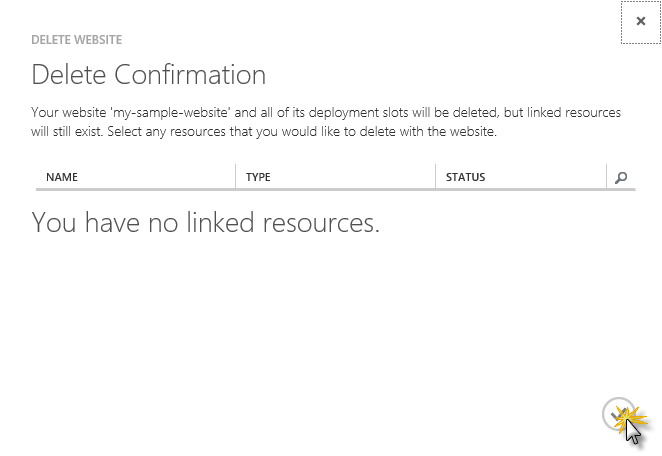
**Note:** It is good practice to cleanup any resources that will not be used. To delete the demo website just created, follow these steps:

* + Click **DASHBOARD** at the top of the page.
  + Click **DELETE** at the bottom of the page.

[Clicking Delete website](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/clicking-delete-website.png?raw=true)

Clicking Delete

* + In the **Delete Confirmation** dialog that pops up, click the **checkmark** button.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-management-portal/images/delete-confirmation-dialog.png?raw=true)

Delete Confirmation

After a few moments you should see a notification indicating the website was deleted. The website will not be listed under **WEBSITES** either.

#### Summary

In this lab you have seen the Azure Management Portal, starting by the basic layout of the hub page, moving to the creation and management of resources. Finally you have explored some of the features that the portal provides.

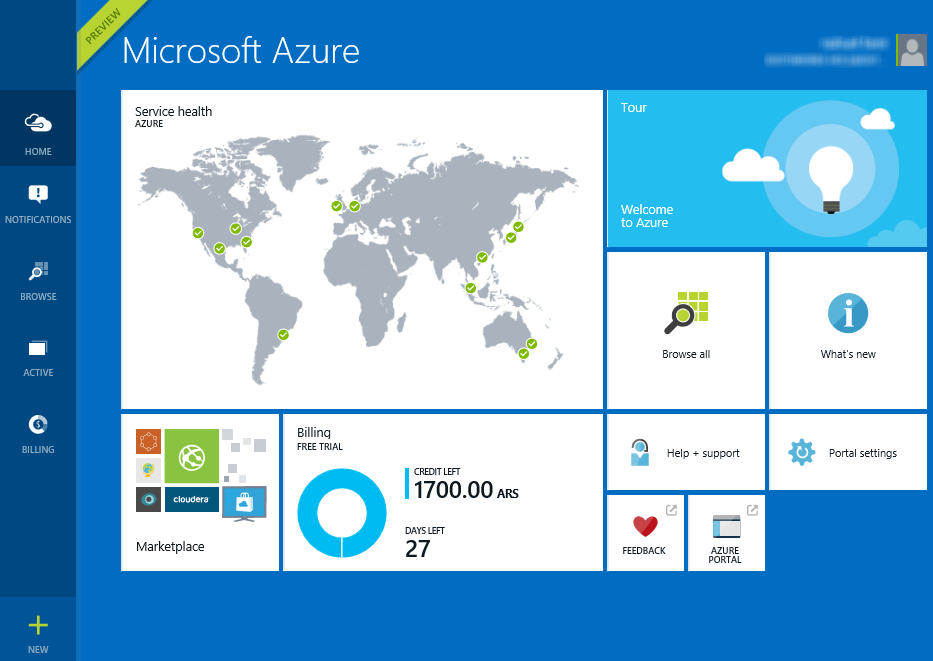
# Lab 12 Creating a Web Site + SQL (Preview Portal)

Historically, managing a resource (a user-managed entity such as a database server, database or web site) in Microsoft Azure required you to perform operations against one resource at a time. When developing for the cloud today, we are often managing individual resources (databases, storage, cloud services, virtual machines, and so on). It is left up to us, as cloud developers and IT professionals, to piece these resources together in a meaningful way and manage them over time. The Microsoft Azure Preview portal was designed to bring together all of the individual resources of an application into a consolidated view. Resource group is a new concept in Azure that serves as the lifecycle boundary for all of its resources.

In this task, you will learn about the preview portal and how to create a new Web Site and a SQL Server using it.

1. Open a browser and browse to [http://portal.azure.com](http://portal.azure.com/) and log in using your credentials.
2. The first thing you will see is the **Startboard**. This is your home page, where you can see dynamic data from your resources and all the details you care about. You can customize it as you see fit.

**Note:** You can right-click the tiles of the Startboard to customize it. You can pin or unpin tiles and change their size.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/startboard.png?raw=true)

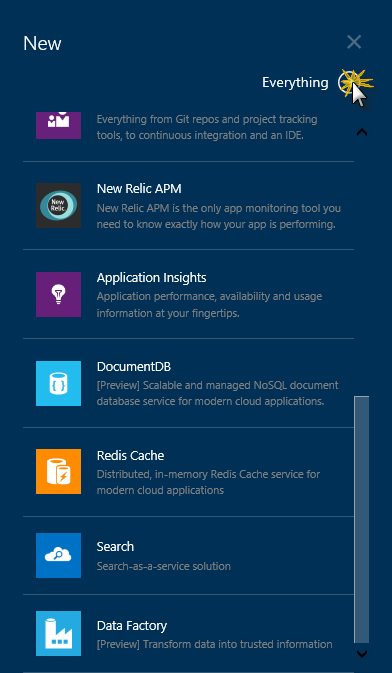
Your Home Page: The Startboard

1. On the left side, you will see the **Hub Menu**. This is the navigation menu where you can access all of your resources and options. Click the **New** button at the bottom of the **Hub Menu**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/creating-a-new-resource.png?raw=true)

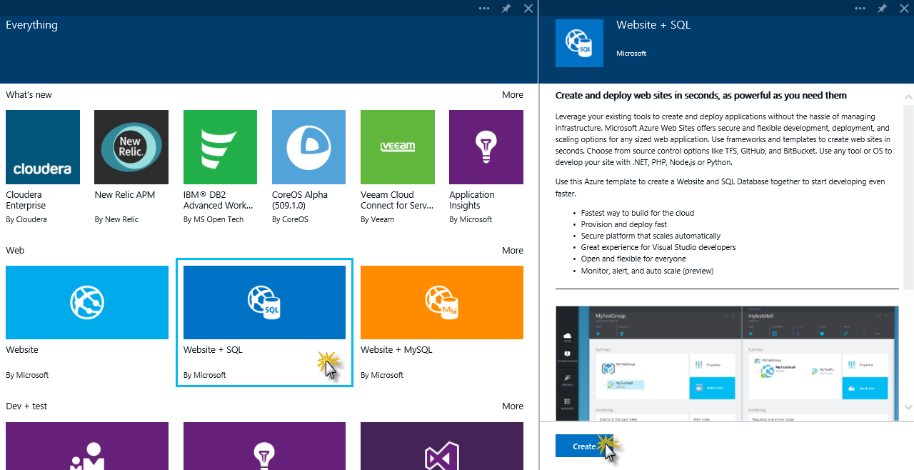
Creating a new resource

1. A panel is displayed with different options. You can choose one of the options to create a new resource. Click the **Everything** button to see all the available options.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/displaying-resource-types.png?raw=true)

Displaying every resource type

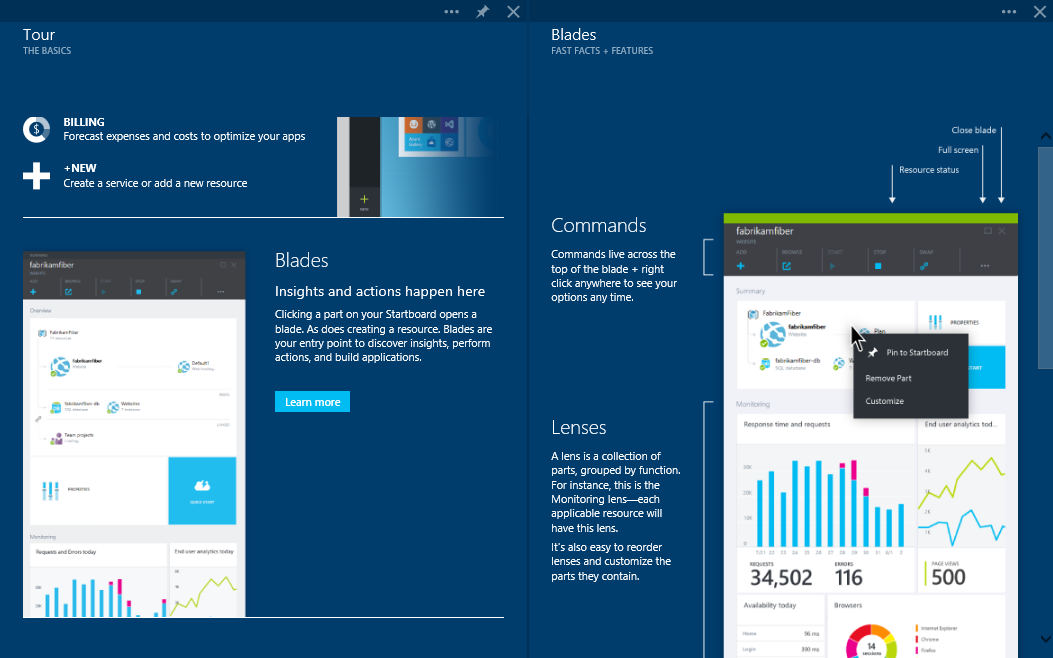
1. Scroll down to the **Web** category, and select **Website +SQL**. Then click **Create**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/selecting-website-sql.png?raw=true)

Selecting Website + SQL

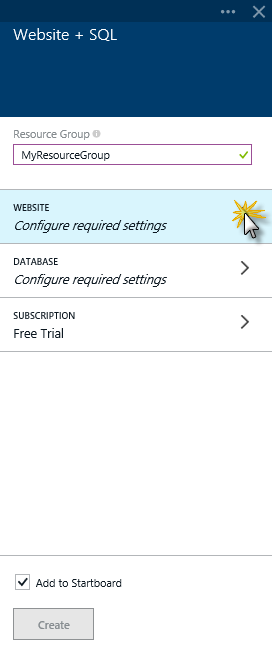
A blade is opened. Blades are your entry point to discovering insights, performing actions and building applications. This particular blade collects input from you to create a new **Website**.

**Note:** For more information about blades, you can click the **Tour** tile on your **Startboard**. On the **Tour** blade, scroll down to the bottom and click **Learn more**. A new blade is opened with further information. You can continue the **Tour** to learn the basics of Blades, Commands, Lenses and more.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/tour.png?raw=true)

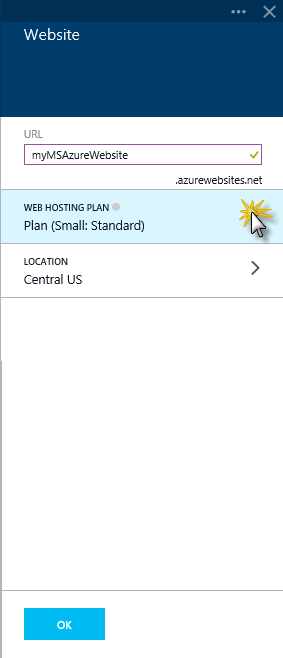
1. When you create an application that consists of several resources working together (like in this example, a Website + SQL), it is always created in its own resource group so that you can manage the lifecycle of all related assets. Choose a name for the **Resource Group**, for example MyResourceGroup, and click the **Website** option.

**Note:** Resource group names can only contain letters, numbers, periods, underscores and dashes.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/new-resource-group.png?raw=true)

New Resource Group

1. Another blade is opened which displays the options to create a new **Website**. Select a URL for your Website, for example myMSAzureWebsite. Take into account that this name must be unique. Click the **Web Hosting Plan** option.

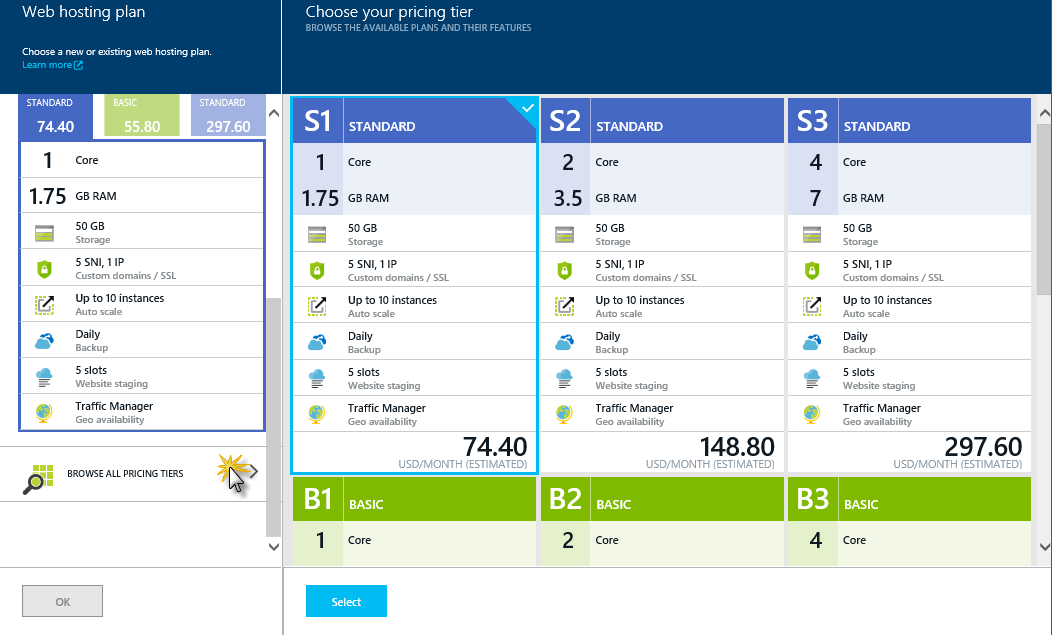
[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/changing-the-web-hosting-plan.png?raw=true)

Changing the Web Hosting Plan

1. Scroll to the bottom of the **Web hosting plan** blade, and click **Browse all pricing tiers**. In the Choose your pricing tier blade, you can choose the hosting plan that fits your needs.

Web hosting plans represent a set of features and capacity that you can share across your Websites. Web hosting plans support several pricing tiers (e.g. Free, Shared, Basic and Standard), each with its own capabilities. There are a couple of differences among these tiers. Plans in the Free and Shared tier provide sites with a shared infrastructure, meaning that your sites share resources with other customers' sites. Web hosting plans in the Basic and Standard tiers provider sites with a dedicated infrastructure, meaning that only the site or sites you choose to associate with this plan will be running on those resources. In this tier you can configure your web hosting plan to use one or more virtual machine instances. As we are going to use the default web hosting plan, just close this blade.

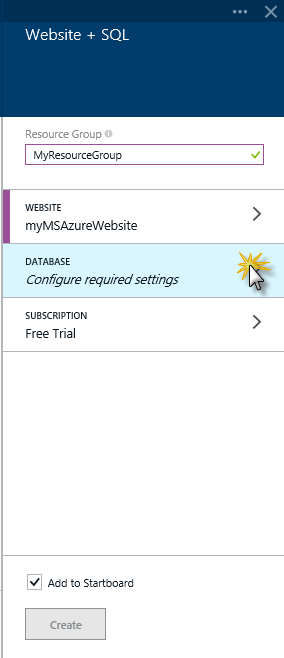
**Note:** For all tiers (except 'Shared') you pay one price for the web hosting plan based on the tier and your chosen capacity with no additional charge for each site that uses the plan. Shared web hosting plans are different; due to the nature of the shared infrastructure, you are charged separately for each site in the plan.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/selecting-a-web-hosting-plan.png?raw=true)

Selecting a Web Hosting Plan

1. Click **Ok** to go back to the **Website** blade. You can change or leave the default location for the Website. Click **OK** to go to the previous blade.
2. Click **Database** to change the settings for your new database.

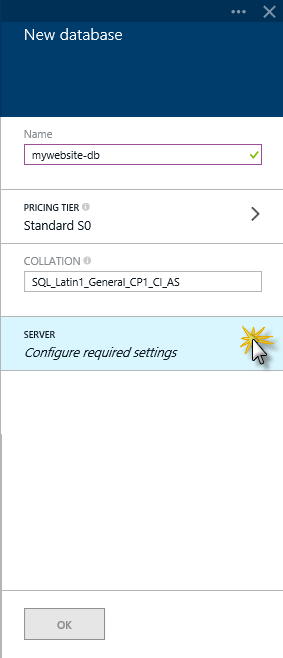
**Note:** If there are any existing databases asociated to the user, the **Database** blade will show up. Select **Create a new Database**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/changing-your-database-settings.png?raw=true)

Changing your database settings

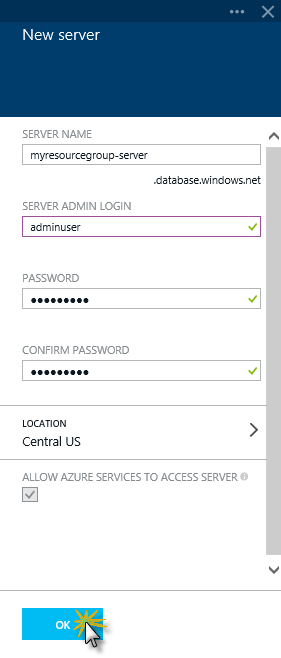
1. Set a name for the database, e.g. mywebsite-db, and click the **Server** option.

**Note:** You can also enter in the **Pricing Tier** section and explore the different pricing tiers.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/database-settings.png?raw=true)

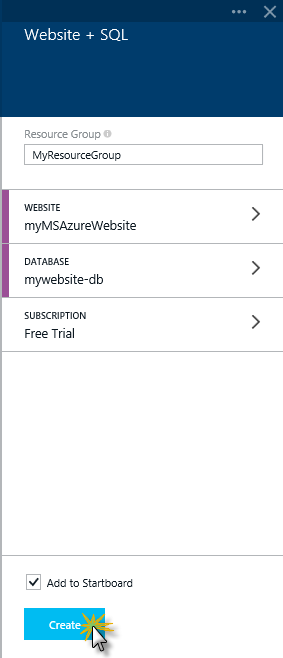
Database Settings

1. Enter the **Server Name**, **Server admin login** and a **Password**. Click **OK** to go back to the **New Database** blade, and click **OK** to close it.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/configuring-the-database-server.png?raw=true)

Configuring the Database Server

1. Now you are ready to create your resource group. Click **Create**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/configured-resource-group.png?raw=true)

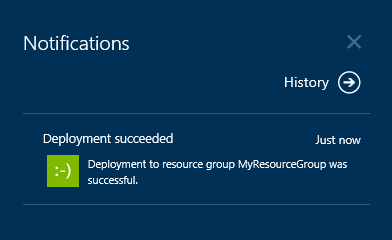
Configured Resource Group

1. You can see when the new resource group is created by accessing the **Notifications** tool. On the **Hub Menu**, click **Notifications**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/notifications.png?raw=true)

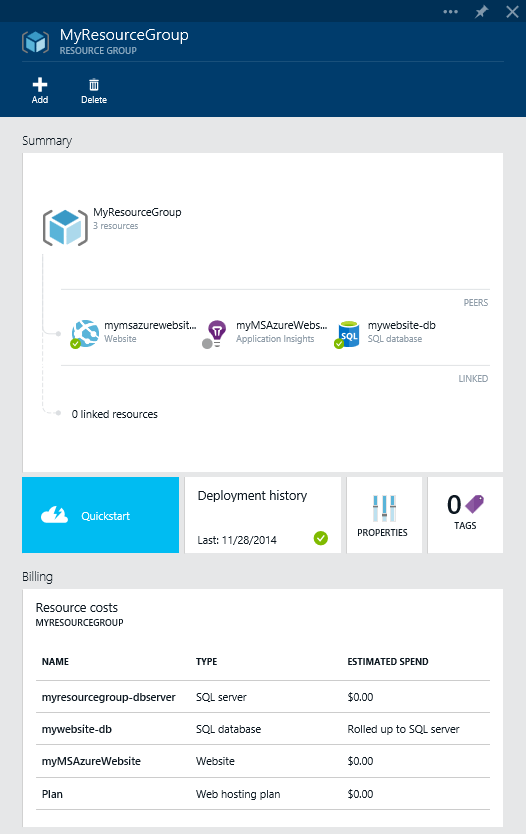
Notifications

1. Once completed, you can click the notification to open the resource group blade.

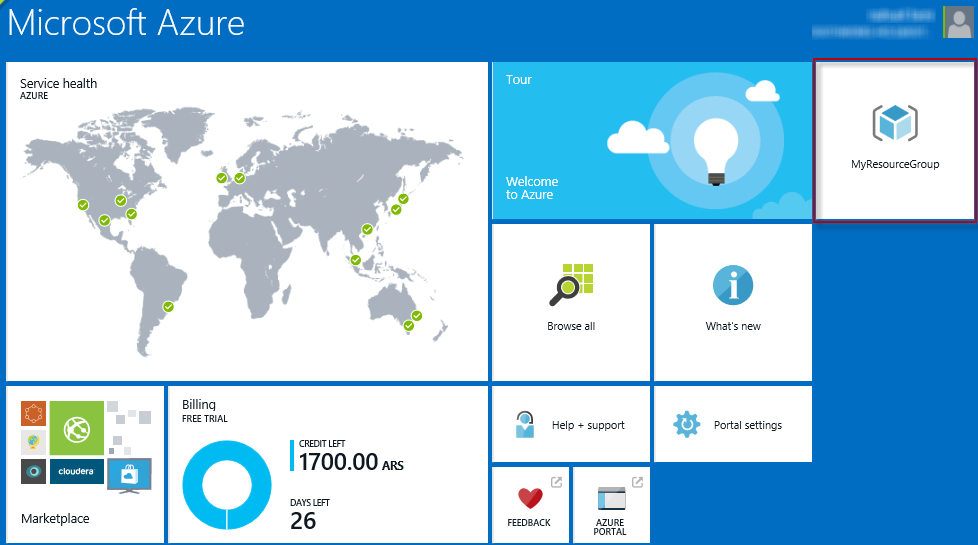
[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/created-resource-group-notification.png?raw=true)

Created Resource Group Notification

1. You created your new resource group, which includes a Website and SQL Server database.

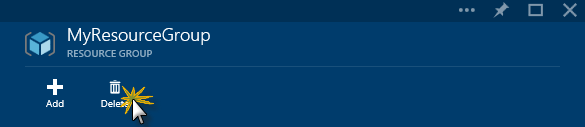
[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/new-resource-group-blade.png?raw=true)

New Resource Group Blade

**Note:** Notice that the recently created resource group was automatically added to the Startboard for easy access. [](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/resource-group-added-to-startboard.png?raw=true)

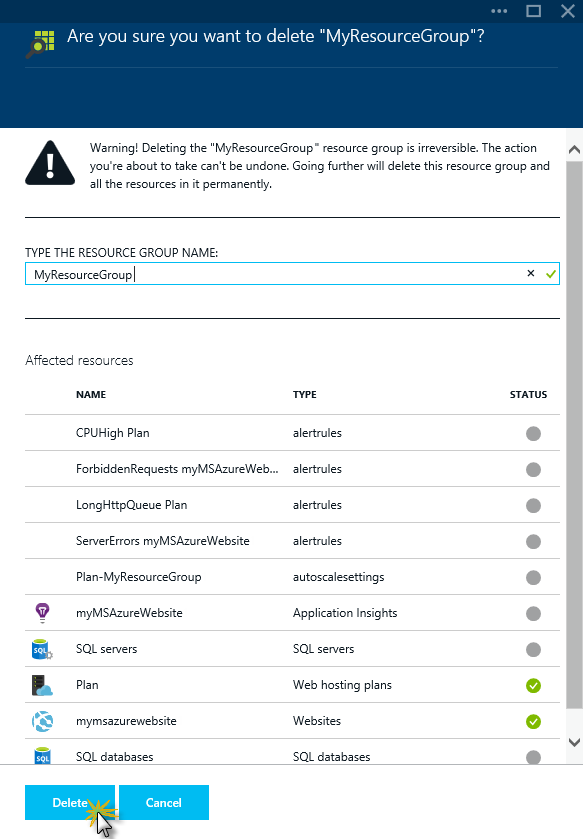
**Note 2:** It is good practice to cleanup any resources that will not be used. To delete the demo resources just created, follow these steps:

* 1. In the Resource Group, click **DELETE** at the top of the page.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/clicking-delete-resource-group.png?raw=true)

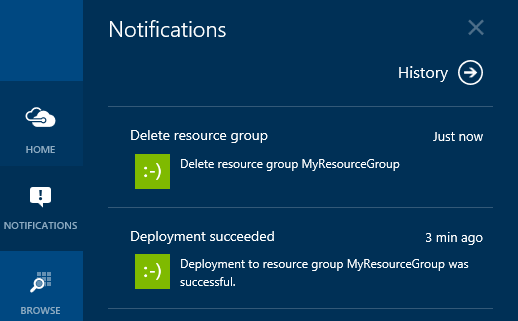
Clicking Delete

* 1. In the Confirmation blade that opens, type the name of the resource group and click the **Delete** button.

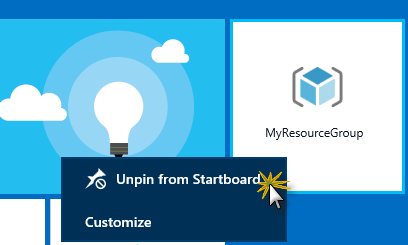
[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/deleting-resource-group-confirmation.png?raw=true)

Delete Confirmation

After a few moments you should see a notification in the Notifications Hub indicating the resource group was deleted.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/notification-after-resource-group-was-deleted.png?raw=true)

* 1. Click **Home** to navigate to the StartBoard. Once there, find and right-click the tile for the resource group. Click **unpin from Startboard**.

[](https://github.com/Azure-Readiness/HOL-Intro-to-Azure/blob/master/working-with-the-new-portal/Images/unpin-resource-group-from-startboard.png?raw=true)

Unpinning Resource Group from StartBoard The tile is removed.

#### Summary

The new Azure Preview portal offers an exciting look into the future of DevOps. This is a first-of-its-kind experience which brings together all of the individual resources, people, and lifecycle stages of your application into a unified portal. In this lab, you learned about the preview portal and how to create a new resource group by building a Website.

# 13 Many More Labs

## Dan Stolts Blog http://ITProGuru.com/HOL

## Capturing Custom Images Page 31

## ADAL and Visual Studio Page 71

## Configure Azure AD Application Proxy Page 82

## External Authentication with ASP.net Page 92

## Consuming Mobile Services Page 143

## Custom Web API Page 159

## Create Websites using Visual Studio Page 254

## Create Packages to Publish Page 271

## Azure Backup (PowerShell Notes) Page 343

## Getting Started with PowerShell Page 354

## PowerShell Working with Storage Page 359

## PowerShell Working with Websites page 360

## Workflows page 361

## GitHub

https://github.com/Azure-Readiness

## Azure Training

Kit https://github.com/Azure-Readiness/MicrosoftAzureTrainingKit/tree/master/HOLs

## PowerShell DSC

http://blogs.msdn.com/b/powershell/archive/2014/04/03/configuring-an-azure-vm-using-powershell-dsc.aspx

# Revision History

1. 2015/02/10 – Version 1 (no version revision)
2. 2015/12/2 – Change Sponsors, Add Page Numbers (1.0.1)